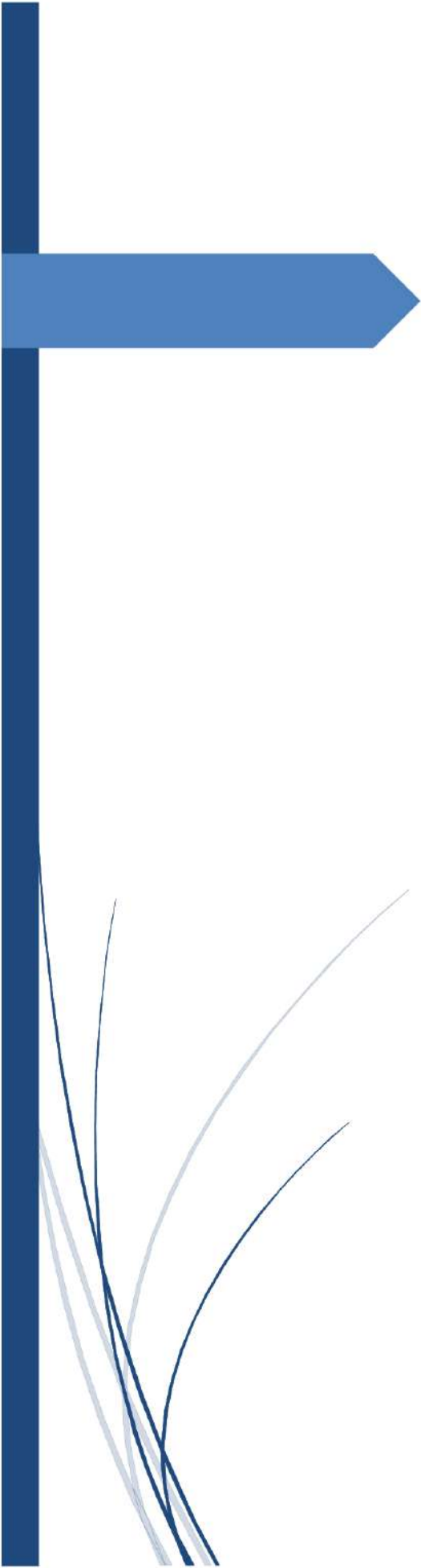




Computer Networks

Practical Book for SYCS class

Prof. Ismail H. Popatia

MAHARASHTRA COLLEGE

Index

Sr No	Date	Practical	Page No	Sign
1		Exploring Networking Commands via Windows CMD / LINUX Terminal	1	
2		Building a Basic Peer-to-Peer Network	3	
3		Static IP Setup with One Server and Two Clients	77	
4		Dynamic IP Allocation with Server and Clients	11	
5		Creating a Mixed Network with Wired and Wireless Devices	15	
6		RIP Version 1 Routing Across Three Routers	25	
7		RIP Version 2 Implementation	38	
8		OSPF Routing and Network Hierarchies	51	
9		BGP for Inter-domain Routing	64	
10		Protocol Analysis with Wireshark	69	

Practical No 1

Aim: Using, linux-terminal or Windows-cmd, execute following networking commands and note the output: ping, traceroute, netstat, arp, ipconfig, getmac, hostname, NSLookUp, pathping, systemInfo

Theory:

- 1) **ping:** ping is a computer network administration software utility used to test the reachability of a host on an Internet Protocol network. It is available for virtually all Operating systems that have networking capability, including most embedded network systems and administration software
- 2) **traceroute:** The traceroute command(tracert) is a utility designed for displaying the time it takes for a packet of information to travel between a host system and the final destination system. This command returns a list of the hops that the data packets take along their path along their way to the destination
- 3) **netstat:**The netstat provides statistics about all active connections so you that we can find out which computers or networks a PC is connected to
Some of the netstat commands commonly used are
 - i) **netstat-in command**
This netstat function shows the state of all configured interfaces.
 - ii) **netstat-a command**
The netstat-a command shows the state of all sockets.
 - iii) **netstat-s**
The netstat-s command shows statistics for each protocol(while the netstat -p command shows the statistics for the specified protocol).
 - iv) **netstat-r**
Another option relevant to performance is the display of the discovered Path Maximum Transmission Unit (PMTU).
- 4) **arp:** The ARP(Address Resolution Protocol) commands are used to view, display, or modify the details/information in an ARP table/cache.
Some of the common arp commands are as follows
 - i) **arp-a:** This command is used to display the ARP table for a particular IPaddress. It also shows all the entries of the ARP cache or table.
 - ii) **arp-g:** Same as the arp-a command.
 - iii) **arp -d:** This command is used to delete an entry from the ARP table for a

- particular interface. To delete an entry, write `arp -d` command along with the IP address in a command prompt to be deleted.
- iv) `arp -s`: This command is used to add the static entry in the ARP table, which resolves the `InetAddr(IP address)` to the `EtherAddr(physical address)`. To add a static entry in an ARP table, we write `arp -s` command along with the IP address and MAC address of the device in a command prompt.
- 5) `ipconfig`: `ipconfig` (Internet Protocol CONFIGuration) is used to display and manage the IP address assigned to the machine. In Windows, typing `ipconfig` without any parameters displays the computer's currently assigned IP, subnet mask and default gateway addresses.
 - 6) `getmac`: `getmac` is a Windows command used to display the Media Access Control (MAC) addresses for each network adapter in the computer.
 - 7) `hostname`: A hostname is a label that is assigned to a device connected to a computer network and it is used to identify the device.
 - 8) `NSlookup`: Using this command we can find the corresponding IP address or domain name system record. The user can also enter a command for it to do a reverse DNS lookup and find the host name for an IP address that is specified.
 - 9) `Pathping`: This command sends multiple echo Request messages to each router between a source and destination, over a period of time, and then computes results based on the packets returned from each router. It can be used to find the routers or links having network problems.
 - 10) `SystemInfo`: This command is used to display detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties.

Click on the link or scan the QR-code for the video demonstration of the practical:

<https://youtu.be/CeMNBxW5LsM>

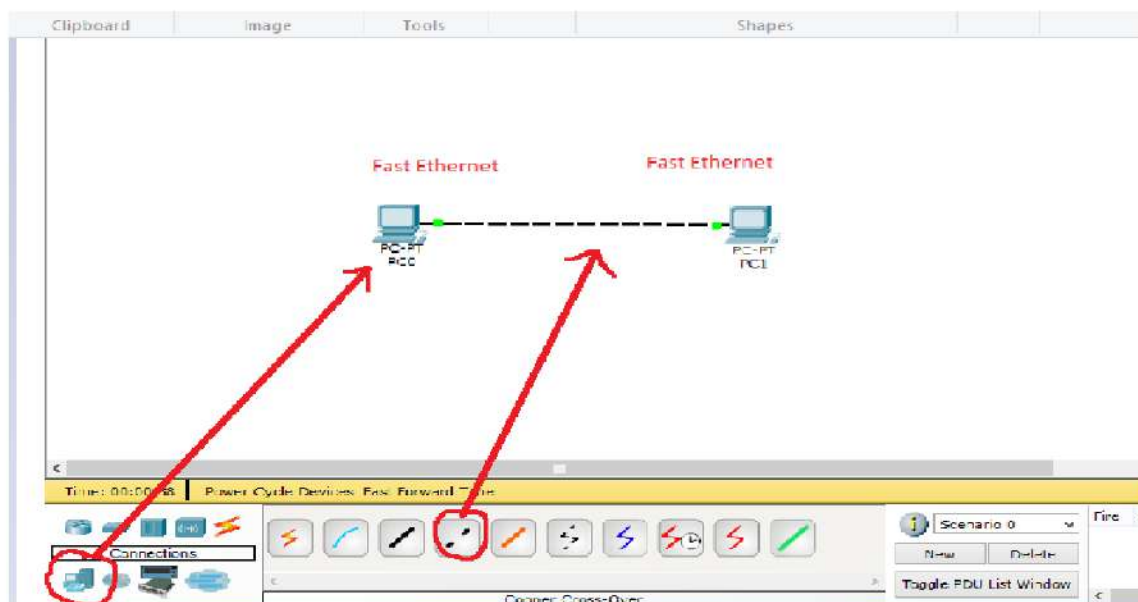


Practical No 2

Aim: Using Packet Tracer, create a basic network of two computers using appropriate network wire through Static IP address allocation and verify connectivity

Theory:

We use the following network to verify the connectivity using Cisco packet tracer



Now we set the ip address of the devices as follows

Hostname	ip Address	Default Gateway
PC0	192.168.1.2	192.168.1.1
PC1	192.168.1.3	192.168.1.1

PC0

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.1.2

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::202:16FF:FEA6:BA6D

Default Gateway

DNS Server

PC1

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.1.3

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

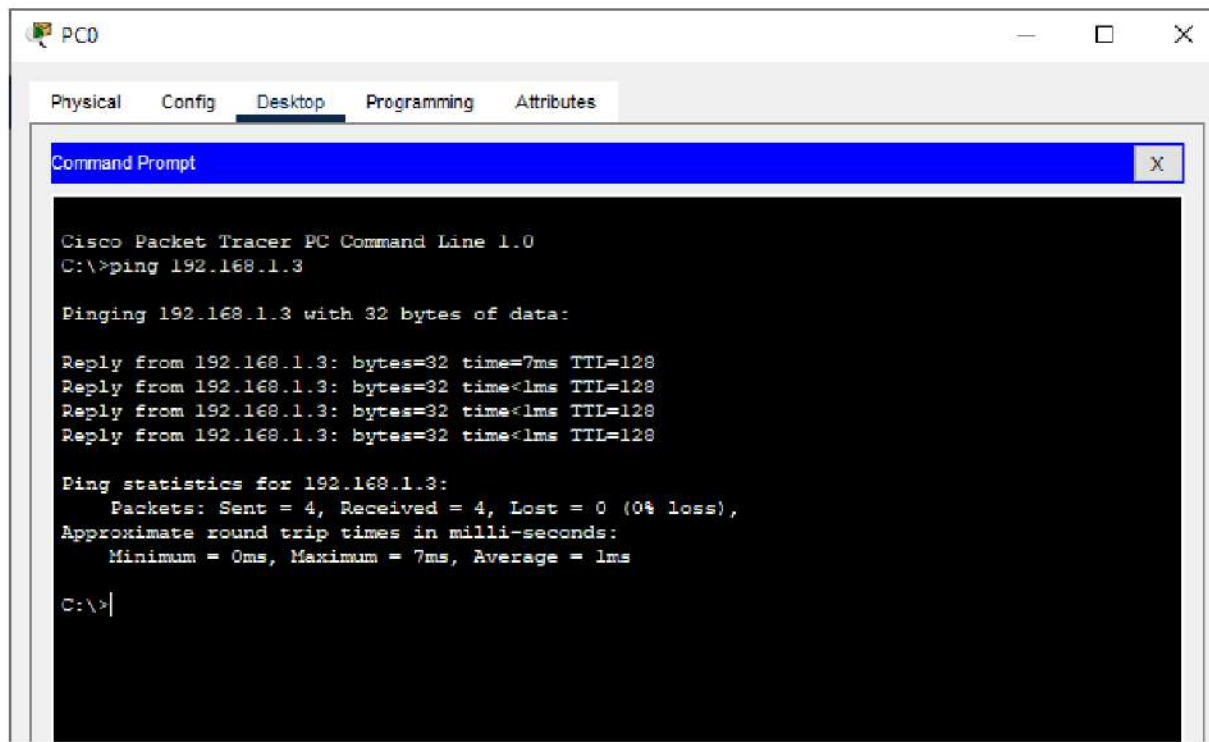
Link Local Address FE80::206:2AFF:FE01:EEDE

Default Gateway

DNS Server

802.1X

In order to check the connectivity we send a ping command from PC0 to PC1 as follows



The screenshot shows a Cisco Packet Tracer interface for PC0. The 'Desktop' tab is selected, displaying a 'Command Prompt' window. The window title is 'Command Prompt' with a close button. The text inside the window is as follows:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=7ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 1ms

C:\>|
```

Result:

Hence the Connectivity between the PCs has been verified.

Click on the link or scan the QR-code for the video demonstration of the practical:

<https://youtu.be/yYYqDgMlXqQ>



Practical No 3

Aim: Using Packet Tracer, create a basic network of one server and two computers using appropriate network wire. Use Dynamic IP address allocation and show connectivity

Theory:

For assigning ip addresses dynamically we use the DHCP protocol

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

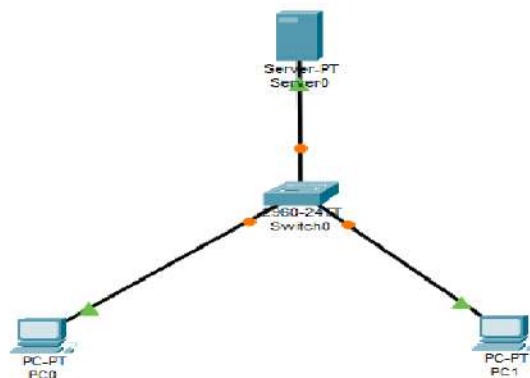
The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it starts up on the network. Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.

DHCP provides the following benefits.

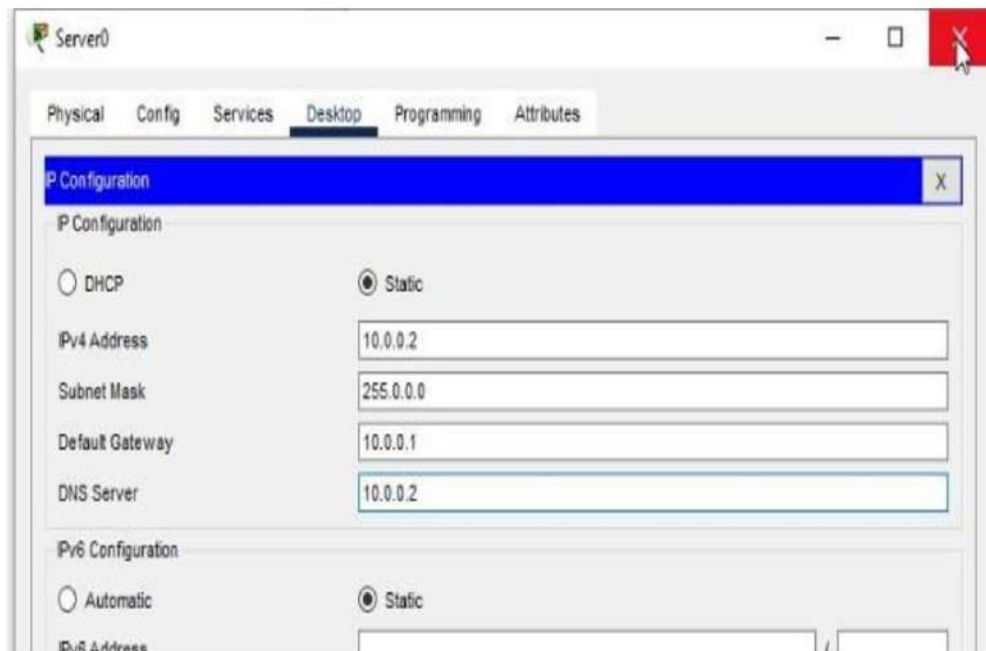
- 1) Reliable IP address configuration. DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time.
- 2) Reduced network administration. DHCP includes the following features to reduce network administration

DHCP runs at the application layer of the Transmission Control Protocol/IP (TCP/IP) stack to dynamically assign IP addresses to DHCP clients and to allocate TCP/IP configuration information to DHCP clients. This includes subnet mask information, default gateway IP addresses and domain name system (DNS) addresses.

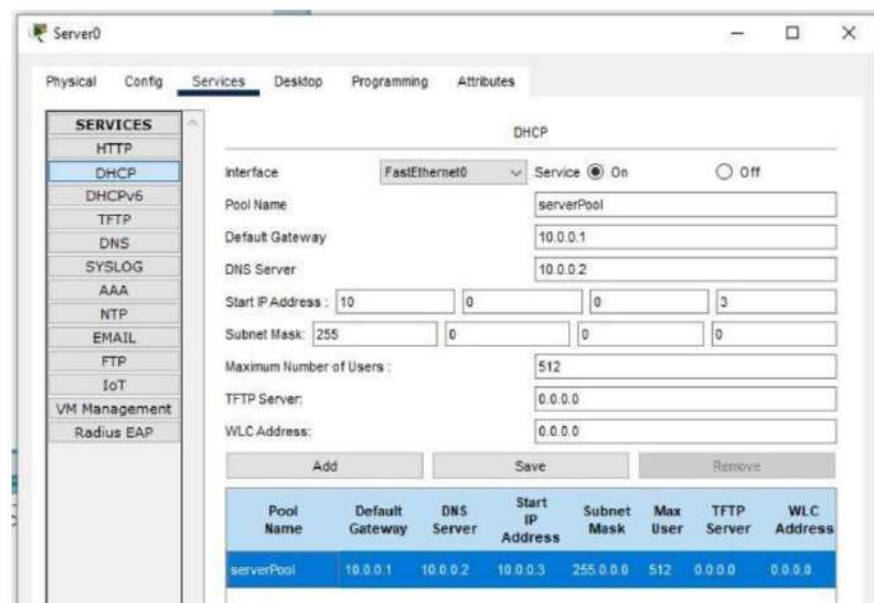
We use the following topology for the present case



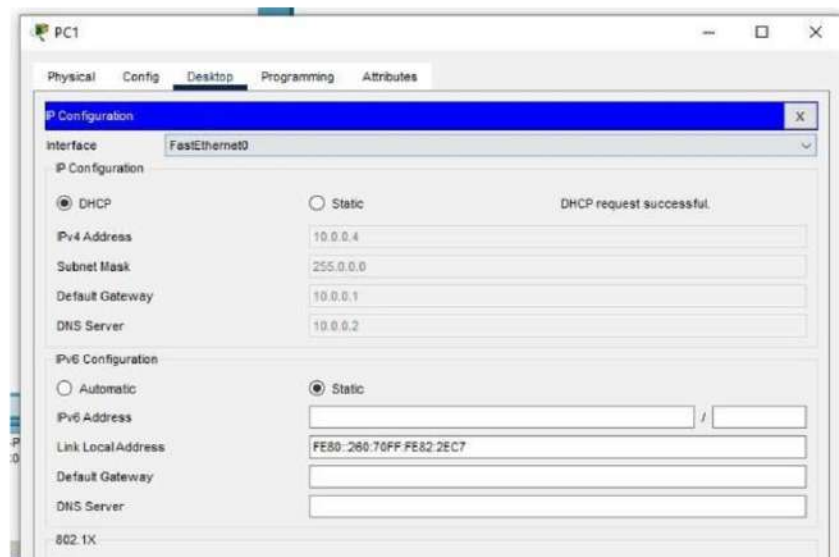
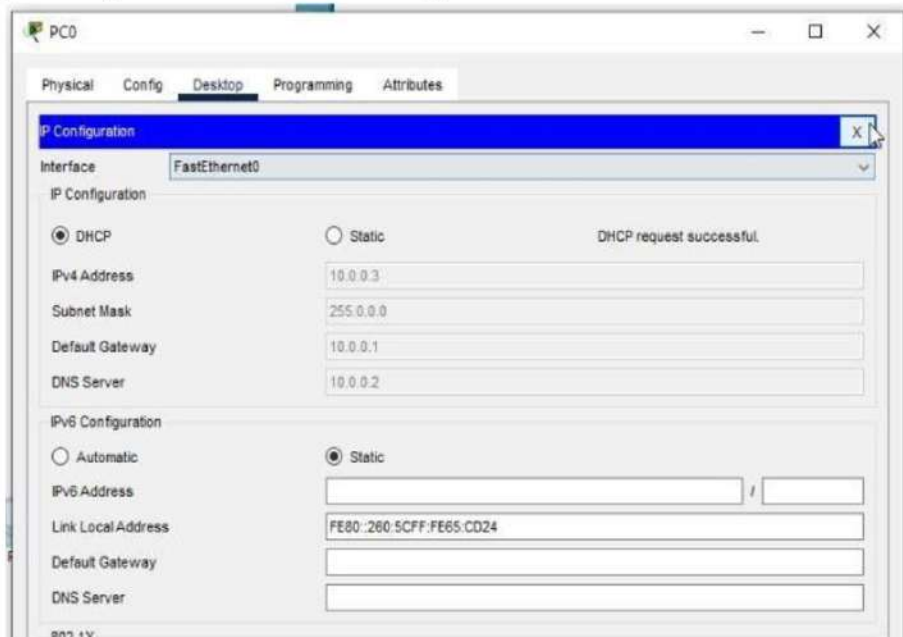
Configuring the Server:



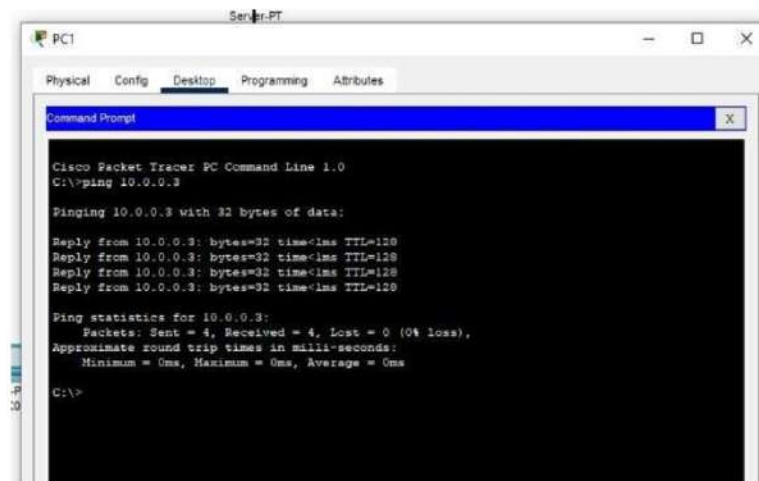
Enabling and setting the DHCP Service on the Server:



Verifying the Dynamic Addressing on both the PCs:



Checking the connectivity:



```
PC1
Physical  Config  Desktop  Programming  Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.3

Pinging 10.0.0.3 with 32 bytes of data:

Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Result:

Hence the Connectivity between the PCs has been verified

Click on the link or scan the QR-code for the video demonstration of the practical:

https://youtu.be/Jnj8c_15AiE



Practical No 4

Aim: Using Packet Tracer, create a basic network of one server and two computers and two mobile / movable devices using appropriate network wire. And verify the connectivity

Theory:

A Wireless Access Point (WAP) is a networking device that allows wireless- capable devices to connect to a wired network. Instead of using wires and cables to connect every computer or device in the network, installing WAPs is a more convenient, more secure, and cost-efficient alternative.

Setting up a wireless network provides a lot of advantages and benefits for you and your small business.

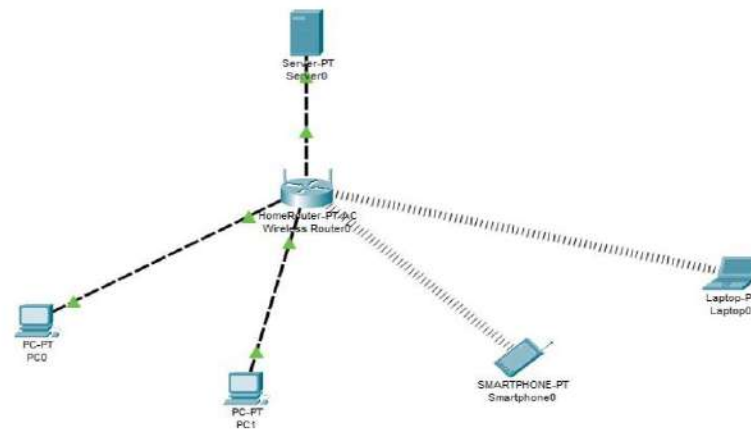
- 1) It is easier to set up compared to setting up a wired network.
- 2) It is more convenient to access.
- 3) It is less complicated to add new users in the network.
- 4) It gives users more flexibility to stay online even when moving from one area in the office to another.
- 5) Guest users can have Internet access by just using a password.
- 6) Wireless network protection can be set up even if the network is visible to the public by configuring maximum wireless security.
- 7) Segmentation of users, such as guests and employees, is possible by creating Virtual Local Area Networks (VLANs) to protect your network resources and assets.

There are different purposes of setting up a wireless network using a WAP.

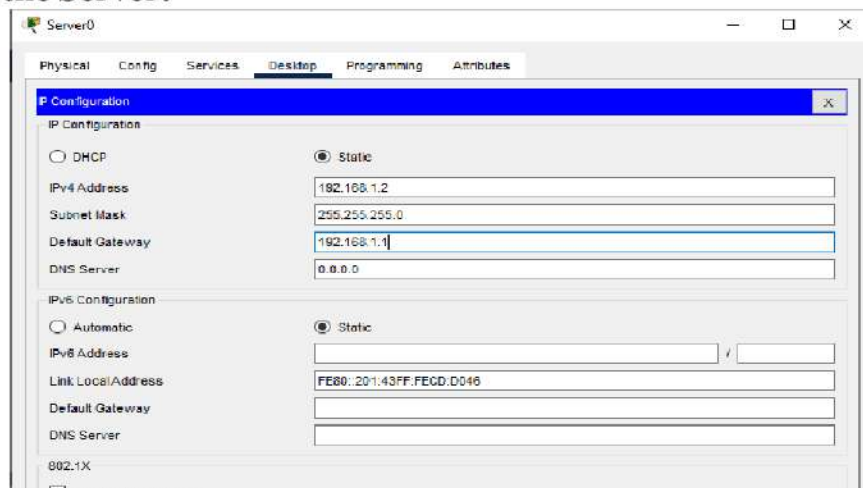
With a WAP, the following can be done:

- 1) Create a wireless network within your existing wired network.
- 2) Extend the signal range and strength of your wireless network to provide complete wireless coverage and get rid of dead spots especially in larger office spaces or buildings.
- 3) Accommodate wireless devices within a wired network.
- 4) Configure the settings of your wireless access points in one device.

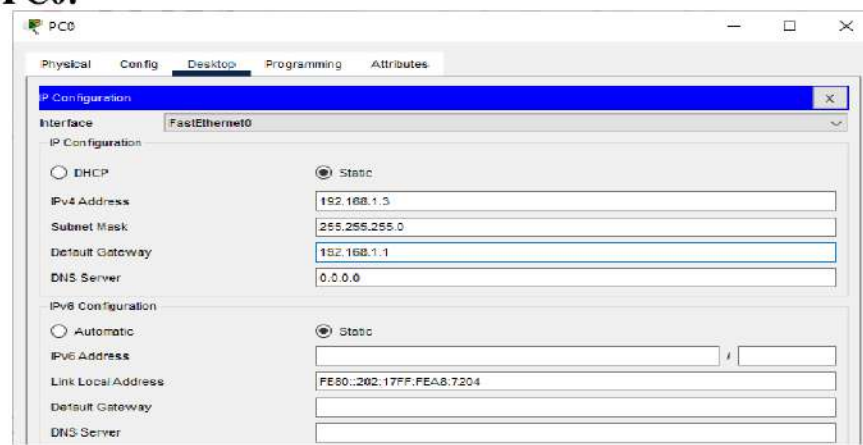
For the present case we use the following topology



Configure the Server:



Configure PC0:



Configure PC1:

The screenshot shows the configuration window for PC1. The 'Desktop' tab is selected. Under 'IP Configuration', the 'Interface' is 'FastEthernet0'. The 'Static' radio button is selected. The fields are filled with the following values:

Field	Value
IPv4 Address	192.168.1.4
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0

Below the IPv4 configuration, the IPv6 configuration section shows 'Automatic' selected, with empty fields for IPv6 Address, Link Local Address, Default Gateway, and DNS Server.

Configure Smartphone0:

The screenshot shows the configuration window for Smartphone0. The 'Desktop' tab is selected. Under 'IP Configuration', the 'Interface' is 'Wireless0'. The 'Static' radio button is selected. The fields are filled with the following values:

Field	Value
IPv4 Address	192.168.1.5
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0

Below the IPv4 configuration, the IPv6 configuration section shows 'Static' selected. The fields are filled with the following values:

Field	Value
IPv6 Address	
Link Local Address	FE80::2E0:F9FF:FE12:4387
Default Gateway	
DNS Server	

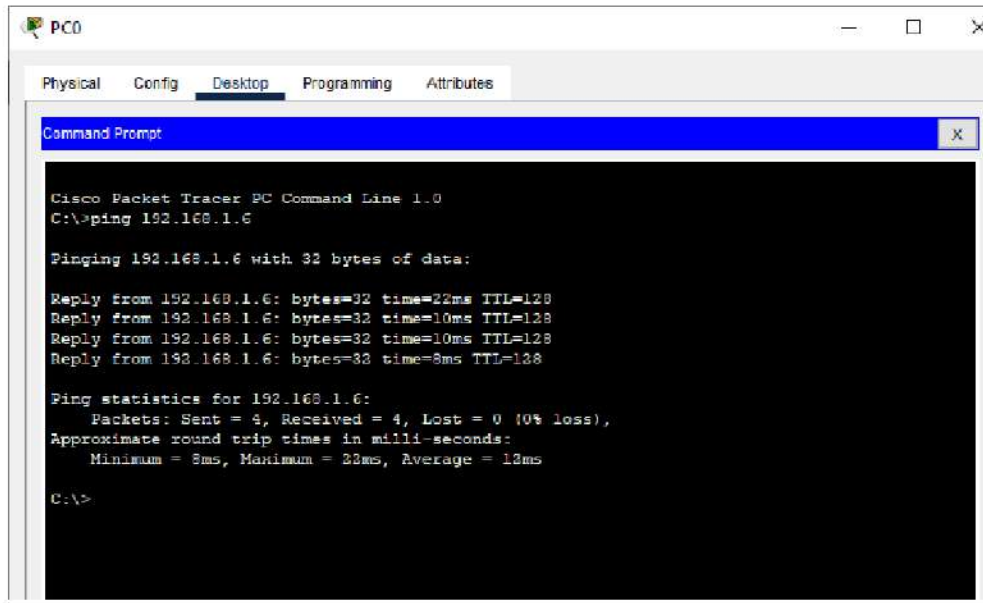
Configure Laptop0:

The screenshot shows the configuration window for Laptop0. The 'Desktop' tab is selected. Under 'IP Configuration', the 'Interface' is 'Wireless0'. The 'Static' radio button is selected. The fields are filled with the following values:

Field	Value
IPv4 Address	192.168.1.6
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0

Below the IPv4 configuration, the IPv6 configuration section shows 'Static' selected. The fields are filled with the following values:

Field	Value
IPv6 Address	
Link Local Address	FE80::20A:F3FF:FE79:78EB
Default Gateway	
DNS Server	

Checking the connectivity (pinging laptop0 from PC0):

The screenshot shows a Cisco Packet Tracer PC Command Line window for PC0. The window has tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, showing a Command Prompt window. The Command Prompt displays the following text:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time=22ms TTL=128
Reply from 192.168.1.6: bytes=32 time=10ms TTL=128
Reply from 192.168.1.6: bytes=32 time=10ms TTL=128
Reply from 192.168.1.6: bytes=32 time=8ms TTL=128

Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 22ms, Average = 12ms

C:\>
```

Similarly the ping message can be checked for all the devices

Result:

Hence the Connectivity of the network has been verified.

Click on the link below or scan the QR-code for the video demonstration

<https://youtu.be/zvBKvkY8-nA>



Practical No 5

Aim: Using Packet Tracer to create a network with three routers with RIPv1 and each router associated network will have minimum three PC and show the connectivity

Theory:

RIP is one of the dynamic routing protocols and the first distance-vector routing protocol that uses the hop count as a routing metric. A lower hop count is preferred.

Each router between the source and destination network is counted as one hop. RIP prevents routing loops by imposing a maximum number of hops on the path between source and destination.

In RIP, Every 30 seconds, each router broadcasts its entire routing table to its nearest neighbors.

Pros and Cons of RIP Protocol

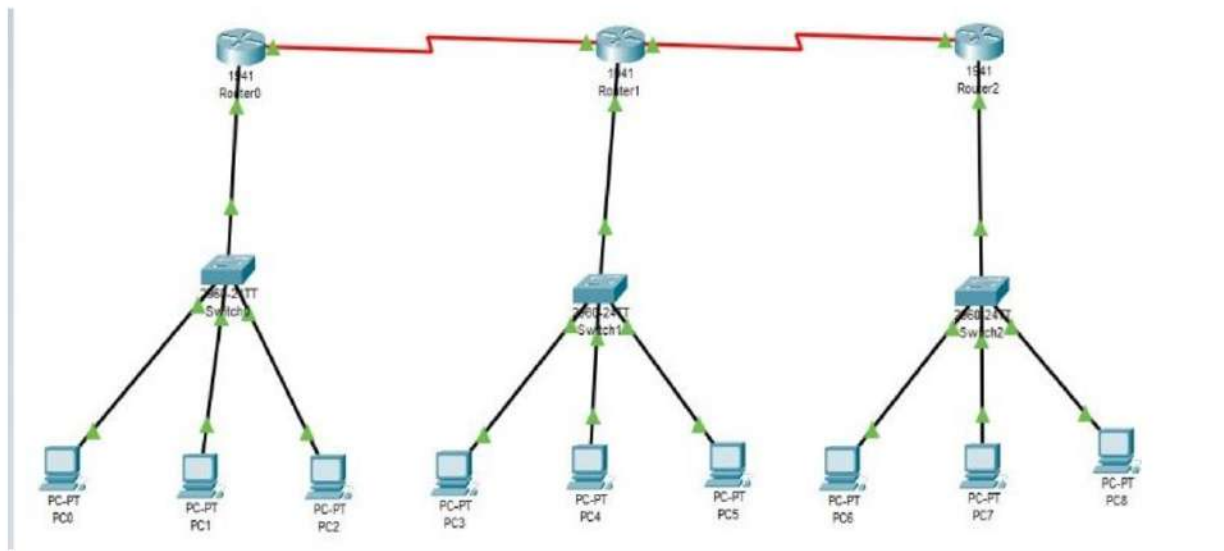
Pros:

1. The RIP protocol is ideal for small networks since it is simple to learn and configure.
2. RIP routing is guaranteed to work with nearly all routers.
3. When the network topology changes, RIP does not require an update.

Cons:

1. RIP does not support variable length subnet masks
2. RIP transmits updates every 30 seconds, which cause traffic and consumes bandwidth.
3. RIP hop counts are restricted to 15, hence any router beyond that distance is deemed infinity and becomes unreachable.
4. The rate of convergence is slow in RIP compared to other routing protocols. When a link fails, finding alternate network paths takes a long time.
5. RIP does not support multiple paths on the same route, which may result in extra routing loops.

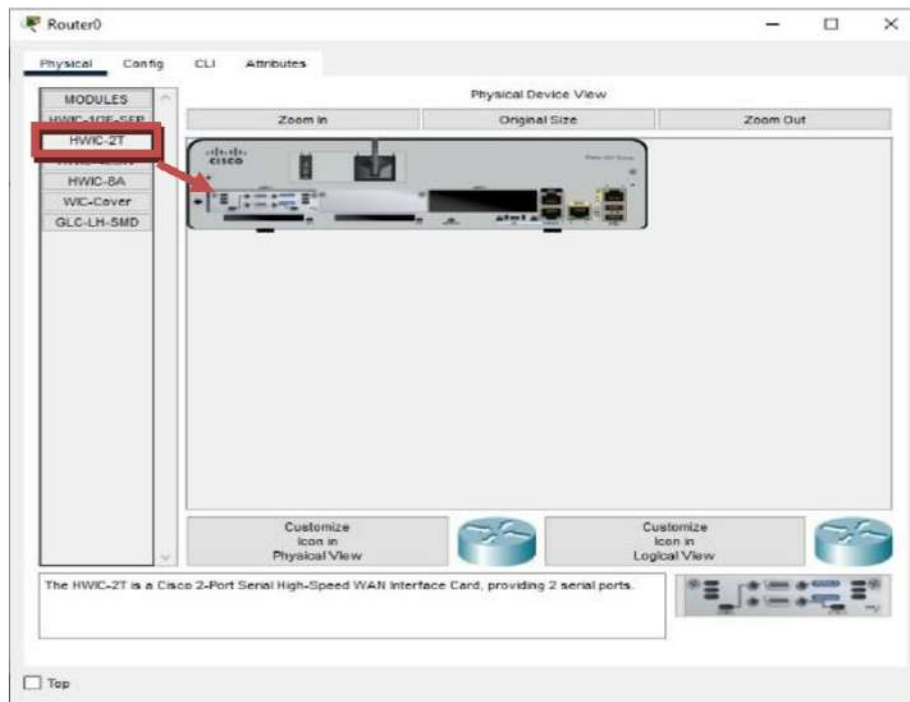
We use the following topology for the present case



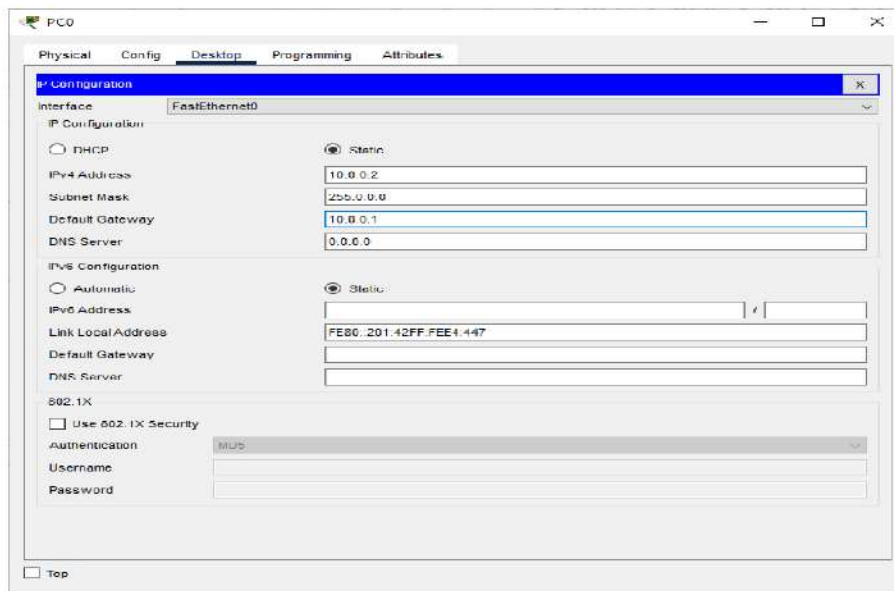
We configure the above network using the following IP addresses

Host	Interface	IP address	Network Address	Default Gateway
Router 0	G0/0	10.0.0.1	10.0.0.0	
	S0/1/0	192.168.0.1	192.168.0.0	
Router 1	G0/0	20.0.0.1	20.0.0.0	
	S0/1/0	192.168.0.2	192.168.0.0	
Router 2	S0/1/1	192.168.1.1	192.168.1.0	
	G0/0	30.0.0.1	30.0.0.0	
	S0/1/1	192.168.1.2	192.168.1.0	
PC0	FastEthernet0	10.0.0.2	10.0.0.0	10.0.0.1
PC1	FastEthernet0	10.0.0.3	10.0.0.0	10.0.0.1
PC2	FastEthernet0	10.0.0.4	10.0.0.0	10.0.0.1
PC3	FastEthernet0	20.0.0.2	20.0.0.0	20.0.0.1
PC4	FastEthernet0	20.0.0.3	20.0.0.0	20.0.0.1
PC5	FastEthernet0	20.0.0.4	20.0.0.0	20.0.0.1
PC6	FastEthernet0	30.0.0.2	30.0.0.0	30.0.0.1
PC7	FastEthernet0	30.0.0.3	30.0.0.0	30.0.0.1
PC8	FastEthernet0	30.0.0.4	30.0.0.0	30.0.0.1

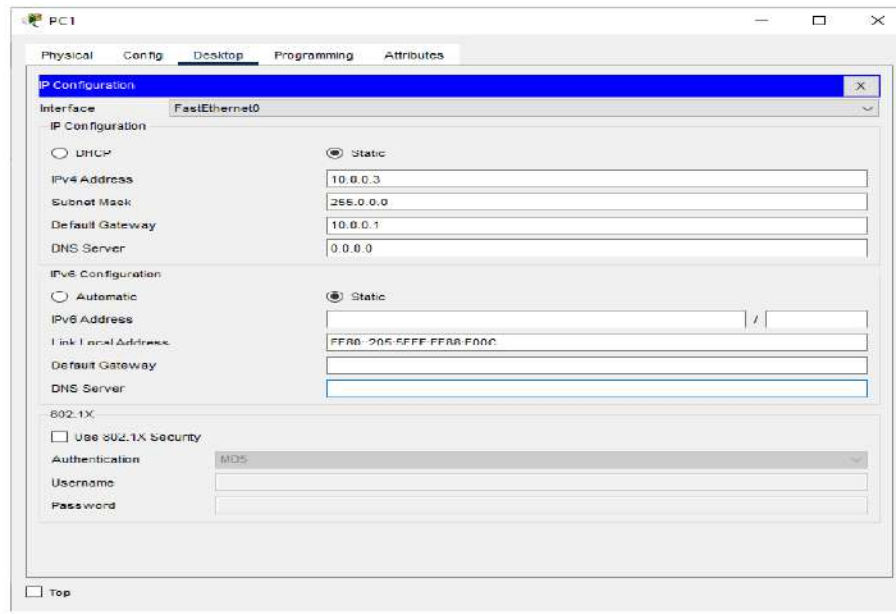
Adding Serial Interface in each Router



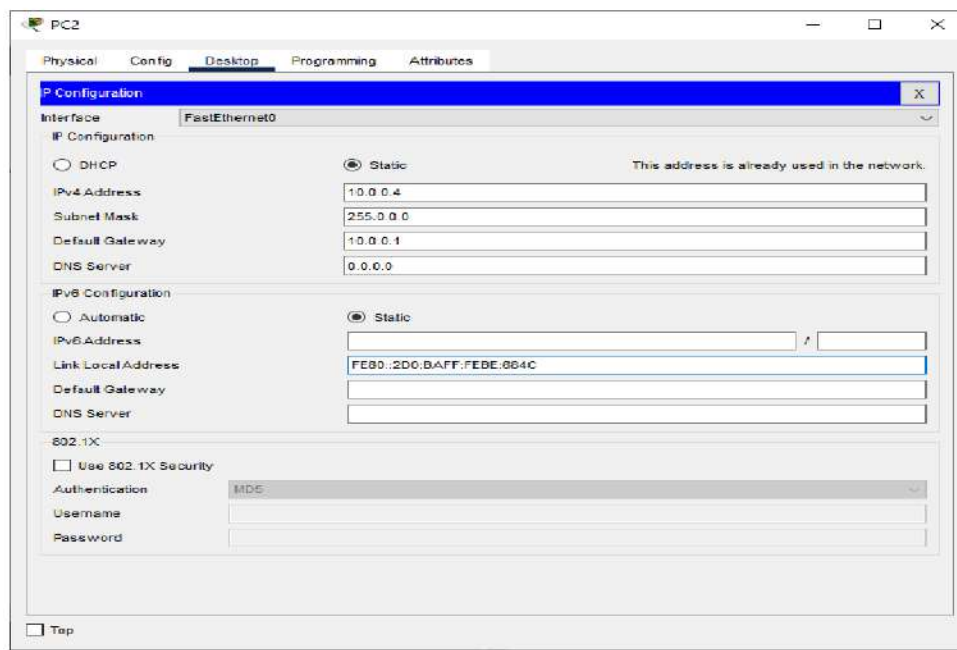
Configuring PC0:

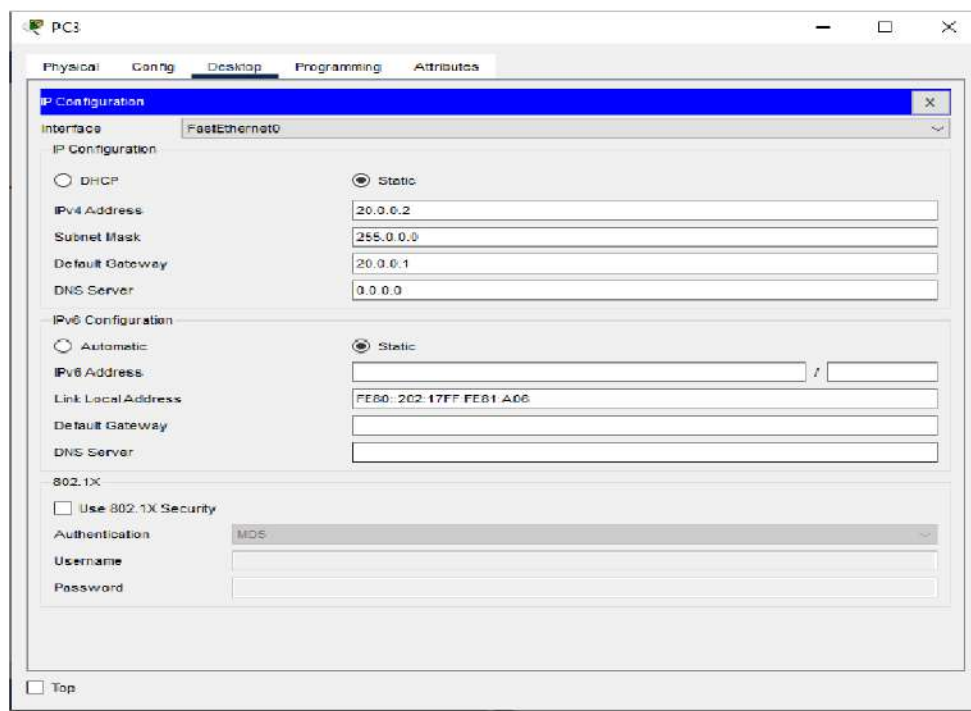


Configuring PC1:

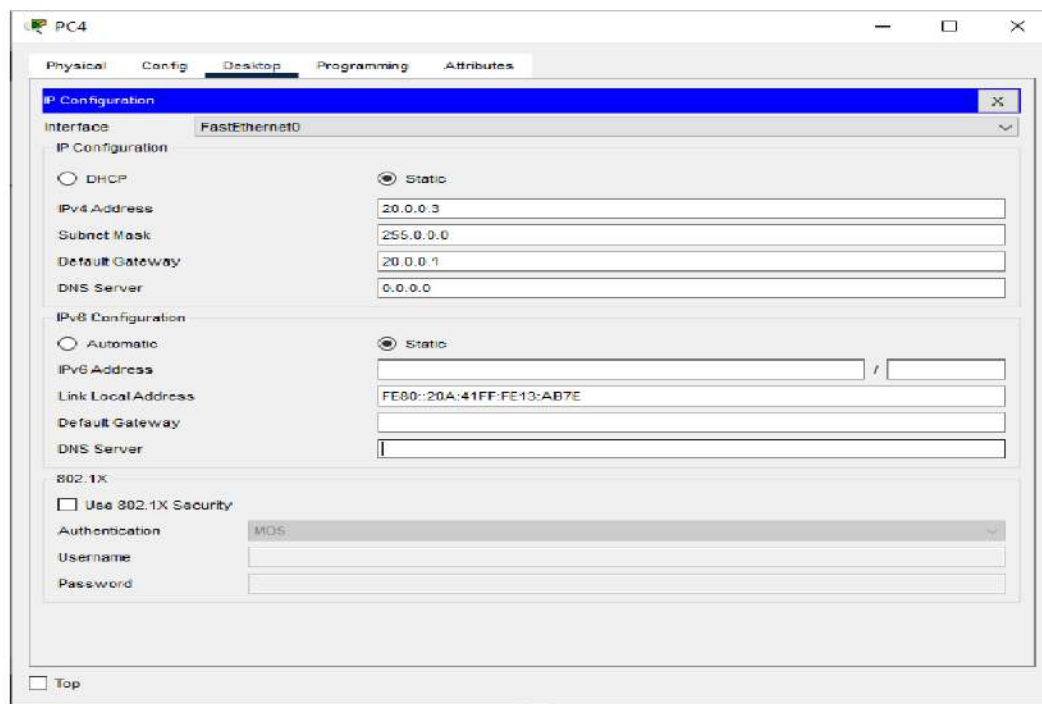


Configuring PC2:





Configuring PC4:



PC5

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 20.0.0.4

Subnet Mask: 255.0.0.0

Default Gateway: 20.0.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::2E0:F9FF:FE9D:3AA

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top

Configuring PC6:

PC6

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 30.0.0.2

Subnet Mask: 255.0.0.0

Default Gateway: 30.0.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::2E0:F9FF:FE9A:D3AA

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top

Configuring PC7:

The screenshot shows the configuration window for PC7. The 'Desktop' tab is selected. The 'IP Configuration' section is expanded, showing the 'FastEthernet0' interface. The 'Static' radio button is selected for IP Configuration. The fields are filled with the following values:

Field	Value
IPv4 Address	30.0.0.3
Subnet Mask	255.0.0.0
Default Gateway	30.0.0.1
DNS Server	0.0.0.0

Below the IPv4 configuration, the IPv6 Configuration section is also visible. The 'Static' radio button is selected. The fields are filled with the following values:

Field	Value
IPv6 Address	
Link Local Address	FE80::201:C9FF:FE0C:D846
Default Gateway	
DNS Server	

At the bottom, the 802.1X section is visible. The 'Use 802.1X Security' checkbox is unchecked. The 'Authentication' dropdown is set to 'MD5'. The 'Username' and 'Password' fields are empty.

Configuring PC8:

The screenshot shows the configuration window for PC8. The 'Desktop' tab is selected. The 'IP Configuration' section is expanded, showing the 'FastEthernet0' interface. The 'Static' radio button is selected for IP Configuration. The fields are filled with the following values:

Field	Value
IPv4 Address	30.0.0.4
Subnet Mask	255.0.0.0
Default Gateway	30.0.0.1
DNS Server	0.0.0.0

Below the IPv4 configuration, the IPv6 Configuration section is also visible. The 'Static' radio button is selected. The fields are filled with the following values:

Field	Value
IPv6 Address	
Link Local Address	FE80::260:3EFF:FE25:E1BE
Default Gateway	
DNS Server	

At the bottom, the 802.1X section is visible. The 'Use 802.1X Security' checkbox is unchecked. The 'Authentication' dropdown is set to 'MD5'. The 'Username' and 'Password' fields are empty.

Configuring Router 0 (using the CLI mode)

```
Router>en
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface serial 0/1/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
Router#
```

Configuring Router 1 (using the CLI mode)

```
Router>enable
Router#configure terminal
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 20.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit

Router(config)#interface serial 0/1/0
Router(config-if)#ip address 192.168.0.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit

Router(config)#interface serial 0/1/1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
```

Configuring Router 2 (using the CLI mode)

```

Router>enable
Router#configure terminal
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 30.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit

Router(config)#interface serial 0/1/1
Router(config-if)#ip address 192.168.1.2 255.255.255.0
Router(config-if)#no shutdown

```

Setting the RIPv1 on Router 0

```

Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)#network 10.0.0.0
Router(config-router)#network 192.168.0.0
Router(config-router)#exit

```

Setting the RIPv1 on Router 1

```

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 192.168.0.0
Router(config-router)#network 20.0.0.0
Router(config-router)#network 192.168.1.0
Router(config-router)#exit
Router(config)#
Router#

```

Setting the RIPv1 on Router 2

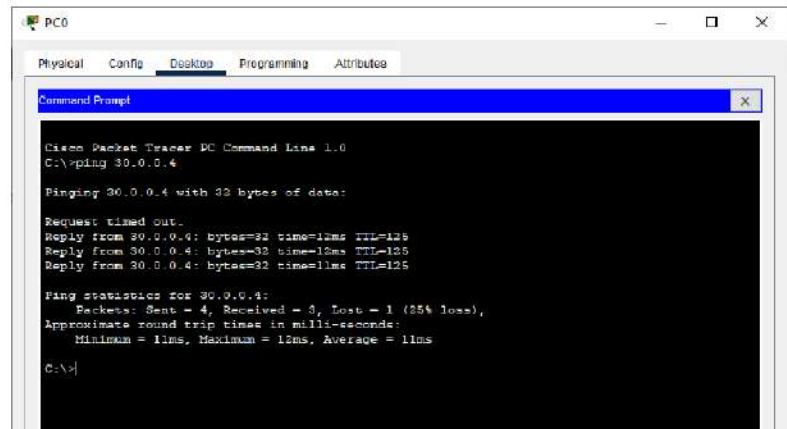
```

Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)#network 192.168.1.0
Router(config-router)#network 30.0.0.0
Router(config-router)#exit
Router(config)#

```

Checking the connectivity by using the ping command

Pinging PC8 (ip address 30.0.0.4) from PC0



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 30.0.0.4

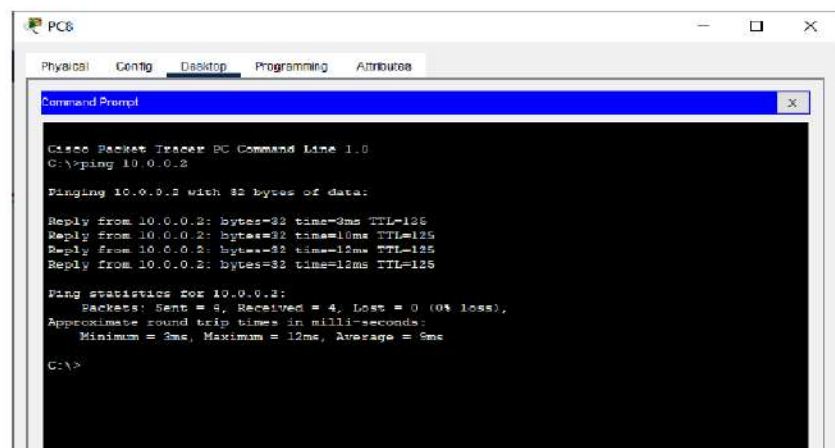
Pinging 30.0.0.4 with 32 bytes of data:

Request timed out.
Reply from 30.0.0.4: bytes=32 time=12ms TTL=125
Reply from 30.0.0.4: bytes=32 time=12ms TTL=125
Reply from 30.0.0.4: bytes=32 time=11ms TTL=125

Ping statistics for 30.0.0.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 12ms, Average = 11ms

C:\>
```

Pinging PC0 (ip address 10.0.0.2) from PC8



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=9ms TTL=125
Reply from 10.0.0.2: bytes=32 time=10ms TTL=125
Reply from 10.0.0.2: bytes=32 time=12ms TTL=125
Reply from 10.0.0.2: bytes=32 time=12ms TTL=125

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 12ms, Average = 9ms

C:\>
```

Result:

Hence the RIPv1 has been studied and verified through the given network

Click on the link below or scan the QR-code for the video demonstration

<https://youtu.be/DLMpobkrDGw>



Practical No 6

Aim: Using Packet Tracer to create a network with three routers with RIPv2 and each router associated network will have minimum three PC and show the connectivity

Theory:

RIPv2 is an enhancement to the original RIP protocol developed in 1994. RIPv2 is also a distance vector routing protocol but has a few enhancements to make it more efficient than RIPv1.

RIPv2 is more efficient than RIPv1, but is not suitable for larger, more complex networks. It simply provides more flexibility on smaller networks.

RIPv2 uses the same routing metric as RIPv1, the hop count. Updates with RIPv2 are sent via multicasts and not broadcasts. RIPv2 can also be configured to do classless routing. When configured for classless routing, RIPv2 will transmit subnet masks when it sends routing updates. This allows for the use of subnetting and discontinuous networks.

RIPv2 allows for authentication to be required for updates. When authentication is enabled, each router is configured with the RIP update password. The password sent with the RIP update must match the password configured on the destination router. If the passwords do not match, then the receiving router will not process the update.

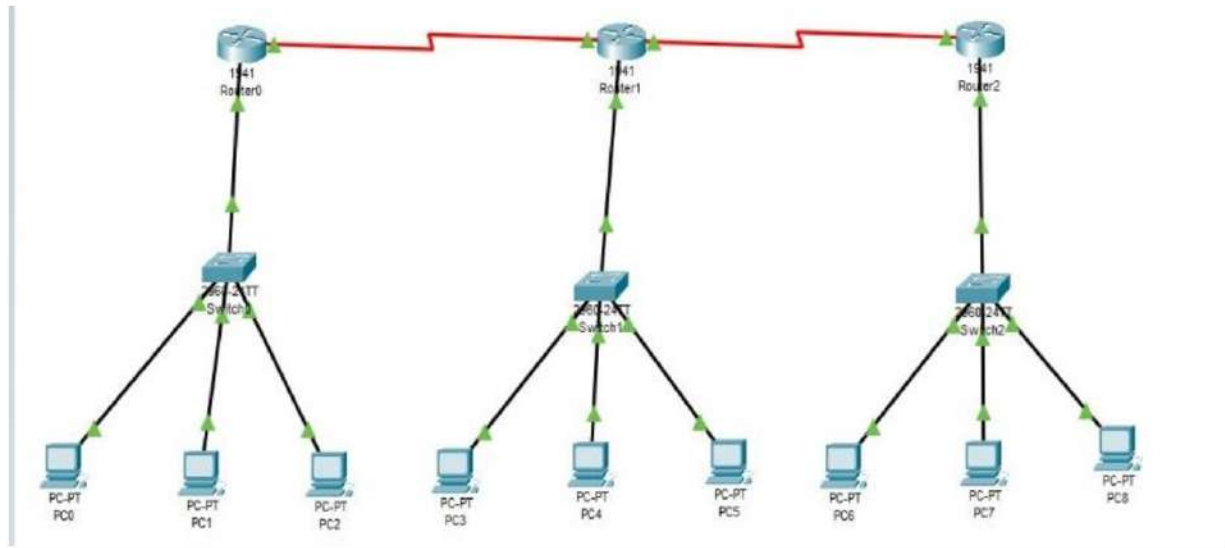
Advantages of RIPv2

- 1) It's a standardized protocol.
- 2) It's VLSM compliant.
- 3) Provides fast convergence.
- 4) It sends triggered updates when the network changes.
- 5) Works with snapshot routing – making it ideal for dial networks.

Disadvantages of RIPv2

- 1) Max hop count of 15, due to the 'count-to-infinity' vulnerability.
- 2) No concept of neighbors.
- 3) Exchanges entire table with all neighbors every 30 seconds (except in the case of a triggered update).

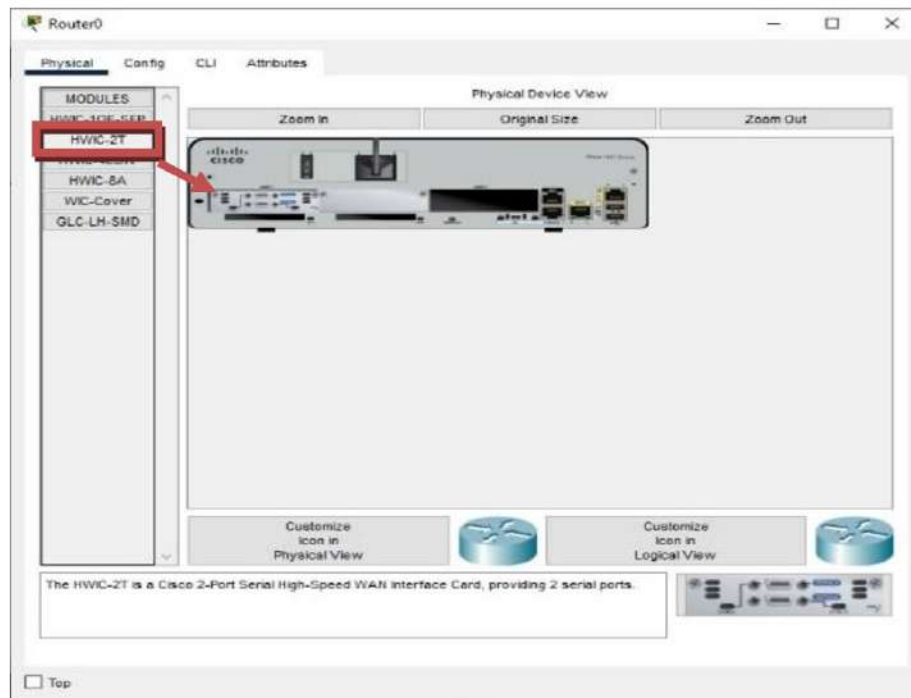
We use the following topology for the present case



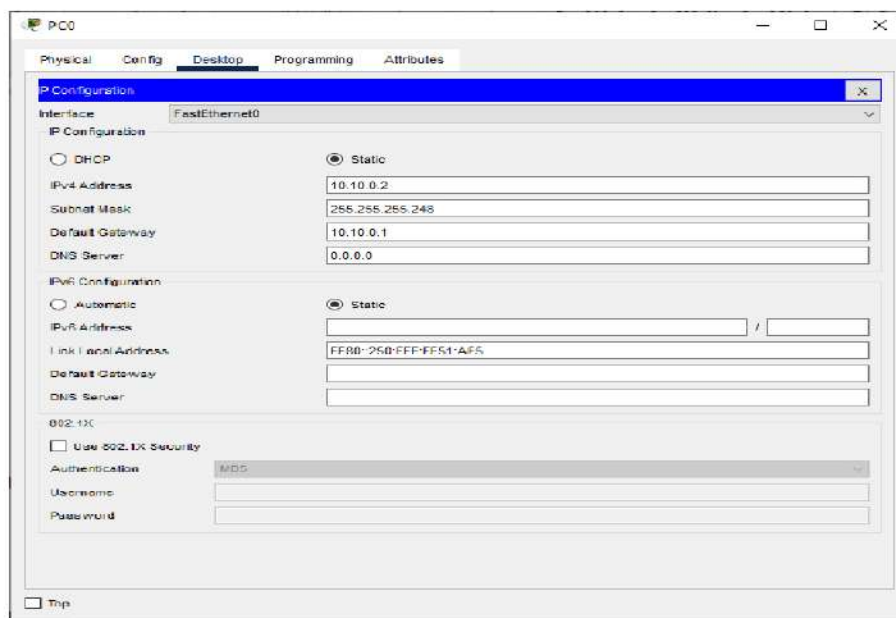
We configure the above network using the following IP addresses

Host	Interface	IP address	Subnet Mask	Network Address	Default Gateway
Router 0	G0/0	10.10.0.1	255.255.255.248	10.10.0.0	
	S0/1/0	192.168.0.1	255.255.255.252	192.168.0.0	
Router 1	G0/0	10.20.0.1	255.255.255.248	10.20.0.0	
	S0/1/0	192.168.0.2	255.255.255.252	192.168.0.0	
	S0/1/1	192.168.1.1	255.255.255.252	192.168.1.0	
Router 2	G0/0	10.30.0.1	255.255.255.248	10.30.0.0	
	S0/1/1	192.168.1.2	255.255.255.252	192.168.1.0	
PC0	FastEthernet0	10.10.0.2	255.255.255.248	10.10.0.0	10.10.0.1
PC1	FastEthernet0	10.10.0.3	255.255.255.248	10.10.0.0	10.10.0.1
PC2	FastEthernet0	10.10.0.4	255.255.255.248	10.10.0.0	10.10.0.1
PC3	FastEthernet0	10.20.0.2	255.255.255.248	10.20.0.0	10.20.0.1
PC4	FastEthernet0	10.20.0.3	255.255.255.248	10.20.0.0	10.20.0.1
PC5	FastEthernet0	10.20.0.4	255.255.255.248	10.20.0.0	10.20.0.1
PC6	FastEthernet0	10.30.0.2	255.255.255.248	10.30.0.0	10.30.0.1
PC7	FastEthernet0	10.30.0.3	255.255.255.248	10.30.0.0	10.30.0.1
PC8	FastEthernet0	10.30.0.4	255.255.255.248	10.30.0.0	10.30.0.1

Adding Serial Interface in each Router



Configuring PC0:



Configuring PC1:

The screenshot shows the 'PC1' configuration window with the 'Desktop' tab selected. The 'IP Configuration' section is expanded, showing settings for the 'FastEthernet0' interface. The 'IP Configuration' section has two radio buttons: 'DHCP' (unselected) and 'Static' (selected). Below these are fields for 'IPv4 Address' (10.10.0.3), 'Subnet Mask' (255.255.255.248), 'Default Gateway' (10.10.0.1), and 'DNS Server' (0.0.0.0). The 'IPv6 Configuration' section also has two radio buttons: 'Automatic' (unselected) and 'Static' (selected). Below these are fields for 'IPv6 Address' (empty), 'Link Local Address' (FE80::2D0:DAFF:FEA4:5B72), 'Default Gateway' (empty), and 'DNS Server' (empty). The '802.1X' section has a checkbox for 'Use 802.1X Security' (unchecked), an 'Authentication' dropdown menu (set to 'MD5'), and fields for 'Username' and 'Password' (both empty). A 'Top' button is located at the bottom left of the window.

Configuring PC2:

The screenshot shows the 'PC2' configuration window with the 'Desktop' tab selected. The 'IP Configuration' section is expanded, showing settings for the 'FastEthernet0' interface. The 'IP Configuration' section has two radio buttons: 'DHCP' (unselected) and 'Static' (selected). Below these are fields for 'IPv4 Address' (10.10.0.4), 'Subnet Mask' (255.255.255.248), 'Default Gateway' (10.10.0.1), and 'DNS Server' (0.0.0.0). The 'IPv6 Configuration' section also has two radio buttons: 'Automatic' (unselected) and 'Static' (selected). Below these are fields for 'IPv6 Address' (empty), 'Link Local Address' (FE80::2D0:ECFF:FE33:A758), 'Default Gateway' (empty), and 'DNS Server' (empty). The '802.1X' section has a checkbox for 'Use 802.1X Security' (unchecked), an 'Authentication' dropdown menu (set to 'MD5'), and fields for 'Username' and 'Password' (both empty). A 'Top' button is located at the bottom left of the window.

Configuring PC3:

The screenshot shows the configuration window for PC3. The 'Desktop' tab is selected. Under 'IP Configuration', the 'Interface' is 'FastEthernet0'. The 'IP Configuration' section has 'Static' selected. The fields are filled with: IPv4 Address: 10.20.0.2, Subnet Mask: 255.255.255.248, Default Gateway: 10.20.0.1, and DNS Server: 0.0.0.0. The 'IPv6 Configuration' section has 'Static' selected, with fields for IPv6 Address, Link Local Address (FE80::2E0:8FFF:FE7E:8379), Default Gateway, and DNS Server. The '802.1X' section has 'Use 802.1X Security' unchecked, and 'Authentication' set to 'MD5'.

Section	Option	Value
IP Configuration	Interface	FastEthernet0
	IP Configuration	Static
	IPv4 Address	10.20.0.2
	Subnet Mask	255.255.255.248
IPv6 Configuration	IPv6 Configuration	Static
	IPv6 Address	
	Link Local Address	FE80::2E0:8FFF:FE7E:8379
	Default Gateway	
802.1X	Use 802.1X Security	Unchecked
	Authentication	MD5
	Username	
Password		

Configuring PC4:

The screenshot shows the configuration window for PC4. The 'Desktop' tab is selected. Under 'IP Configuration', the 'Interface' is 'FastEthernet0'. The 'IP Configuration' section has 'Static' selected. The fields are filled with: IPv4 Address: 10.20.0.3, Subnet Mask: 255.255.255.248, Default Gateway: 10.20.0.1, and DNS Server: 0.0.0.0. The 'IPv6 Configuration' section has 'Static' selected, with fields for IPv6 Address, Link Local Address (FE80::2D0:FFFF:FE8B:2C17), Default Gateway, and DNS Server. The '802.1X' section has 'Use 802.1X Security' unchecked, and 'Authentication' set to 'MD5'.

Section	Option	Value
IP Configuration	Interface	FastEthernet0
	IP Configuration	Static
	IPv4 Address	10.20.0.3
	Subnet Mask	255.255.255.248
IPv6 Configuration	IPv6 Configuration	Static
	IPv6 Address	
	Link Local Address	FE80::2D0:FFFF:FE8B:2C17
	Default Gateway	
802.1X	Use 802.1X Security	Unchecked
	Authentication	MD5
	Username	
Password		

PC5

Physical Config Desktop Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 10.20.0.4

Subnet Mask: 255.0.0.0

Default Gateway: 10.20.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::250:F2FF:FE77:C5E7

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top

Configuring PC6:

PC6

Physical Config Desktop Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 10.30.0.2

Subnet Mask: 255.255.255.248

Default Gateway: 10.30.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::200:CFF:FE40:DCD0

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top

Configuring PC7:

PC7

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 10.30.0.3

Subnet Mask: 255.0.0.0

Default Gateway: 10.30.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: []

Link Local Address: FE80::202:4AFF:FE4A:9D36

Default Gateway: []

DNS Server: []

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username: []

Password: []

☐ Top

Configuring PC8:

PC8

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 10.50.0.4

Subnet Mask: 255.0.0.0

Default Gateway: 10.30.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: []

Link Local Address: FE80::240:BFF:FE65:D944

Default Gateway: []

DNS Server: []

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username: []

Password: []

☐ Top

Configuring IP addresses on Router 0

i) Interface G0/0

The screenshot shows the configuration window for the GigabitEthernet0/0 interface on Router0. The left sidebar has a tree view with categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under INTERFACE, GigabitEthernet0/0 is selected. The main panel shows the configuration for this interface. The Port Status is checked and set to On. Bandwidth is set to 100 Mbps (selected from 1000 Mbps, 100 Mbps, 10 Mbps, and Auto). Duplex is set to Full Duplex (selected from Half Duplex and Full Duplex). The MAC Address is 0090.0C15.A101. The IP Configuration section shows the IPv4 Address as 10.10.0.1 and the Subnet Mask as 255.255.255.248. The Tx Ring Limit is set to 10.

Category	Setting	Value
Port Status	On	☒
Bandwidth	100 Mbps	☒
Duplex	Full Duplex	☒
MAC Address		0090.0C15.A101
IPv4 Address		10.10.0.1
Subnet Mask		255.255.255.248
Tx Ring Limit		10

ii) Interface S0/1/0

The screenshot shows the configuration window for the Serial0/1/0 interface on Router0. The left sidebar has a tree view with categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under INTERFACE, Serial0/1/0 is selected. The main panel shows the configuration for this interface. The Port Status is checked and set to On. Duplex is set to Full Duplex (selected from Half Duplex and Full Duplex). The Clock Rate is set to 1200. The IP Configuration section shows the IPv4 Address as 192.168.0.1 and the Subnet Mask as 255.255.255.252. The Tx Ring Limit is set to 10.

Category	Setting	Value
Port Status	On	☒
Duplex	Full Duplex	☒
Clock Rate		1200
IPv4 Address		192.168.0.1
Subnet Mask		255.255.255.252
Tx Ring Limit		10

Configuring IP addresses on Router 1

i) Interface G0/0

The screenshot shows the configuration window for Router1, specifically for the GigabitEthernet0/0 interface. The left sidebar shows the configuration tree with 'INTERFACE' selected and 'GigabitEthernet0/0' highlighted. The main panel displays the following settings:

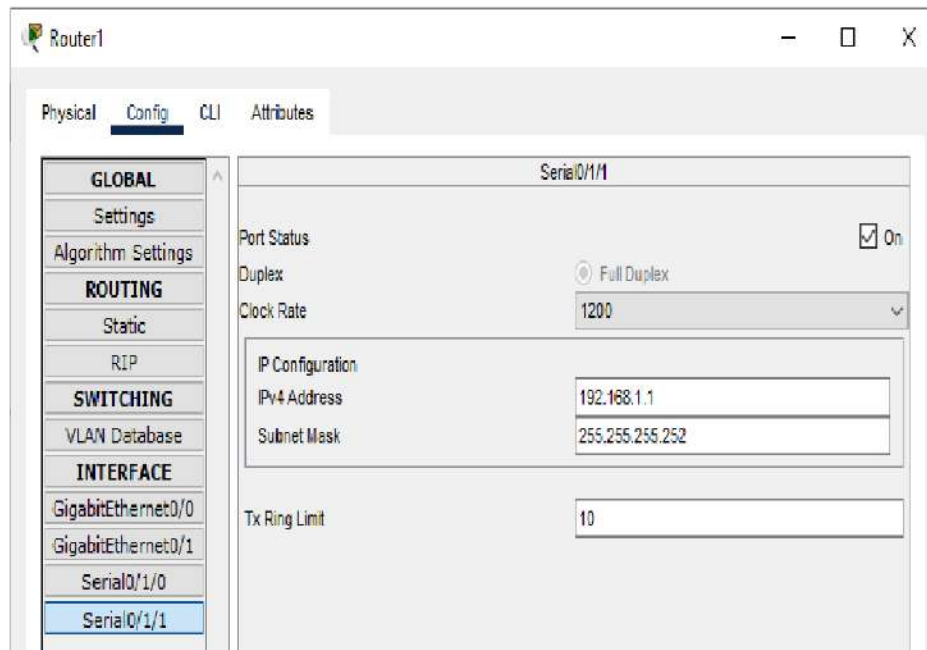
- Port Status:** ☒ On
- Bandwidth:** ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto
- Duplex:** ☐ Half Duplex ☒ Full Duplex ☒ Auto
- MAC Address:** 0001.9870.9B01
- IP Configuration:**
 - IPv4 Address:** 10.20.0.1
 - Subnet Mask:** 255.255.255.248
- Tx Ring Limit:** 10

ii) Interface S0/1/0

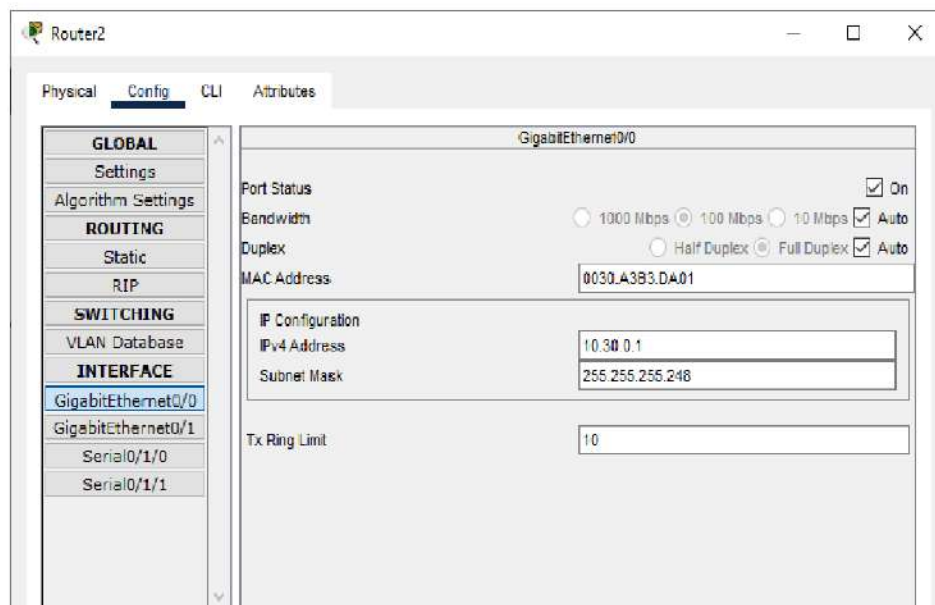
The screenshot shows the configuration window for Router1, specifically for the Serial0/1/0 interface. The left sidebar shows the configuration tree with 'INTERFACE' selected and 'Serial0/1/0' highlighted. The main panel displays the following settings:

- Port Status:** ☒ On
- Duplex:** ☒ Full Duplex
- Clock Rate:** 2000000
- IP Configuration:**
 - IPv4 Address:** 192.168.0.2
 - Subnet Mask:** 255.255.255.252
- Tx Ring Limit:** 10

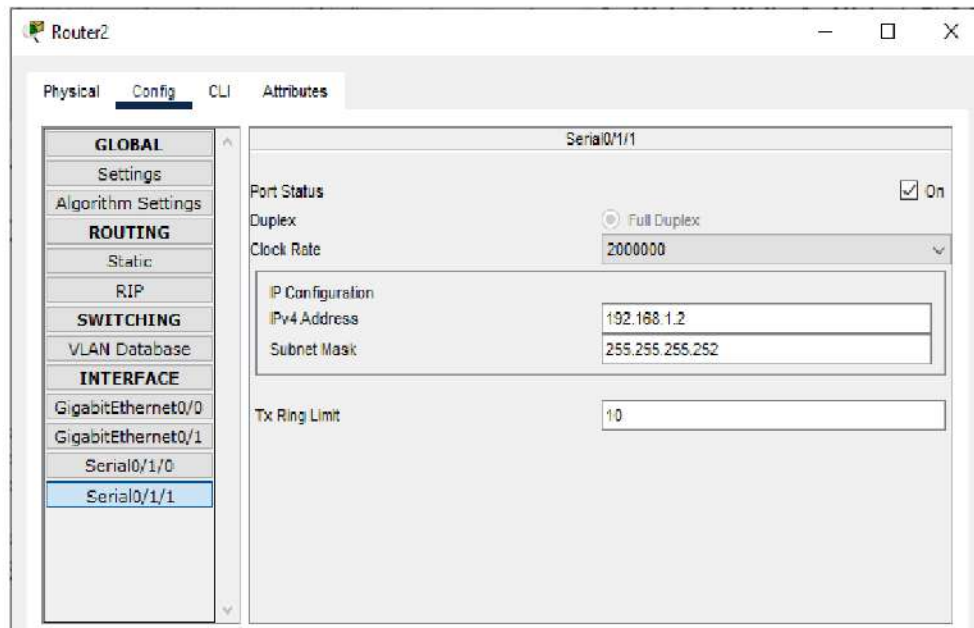
iii) Interface S0/1/1

**Configuring IP addresses on Router 2**

i) Interface G0/0



ii) Interface S0/1/1



Configuring Router 0 for RIPv2 (using the CLI mode)

```
Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 10.10.0.0
Router(config-router)#network 192.168.0.0
Router(config-router)#exit
Router(config)#
```

Configuring Router 1 for RIPv2 (using the CLI mode)

```
Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 10.20.0.0
Router(config-router)#network 192.168.0.0
Router(config-router)#network 192.168.1.0
Router(config-router)#exit
Router(config)#
```

Configuring Router 2 for RIPv2 (using the CLI mode)

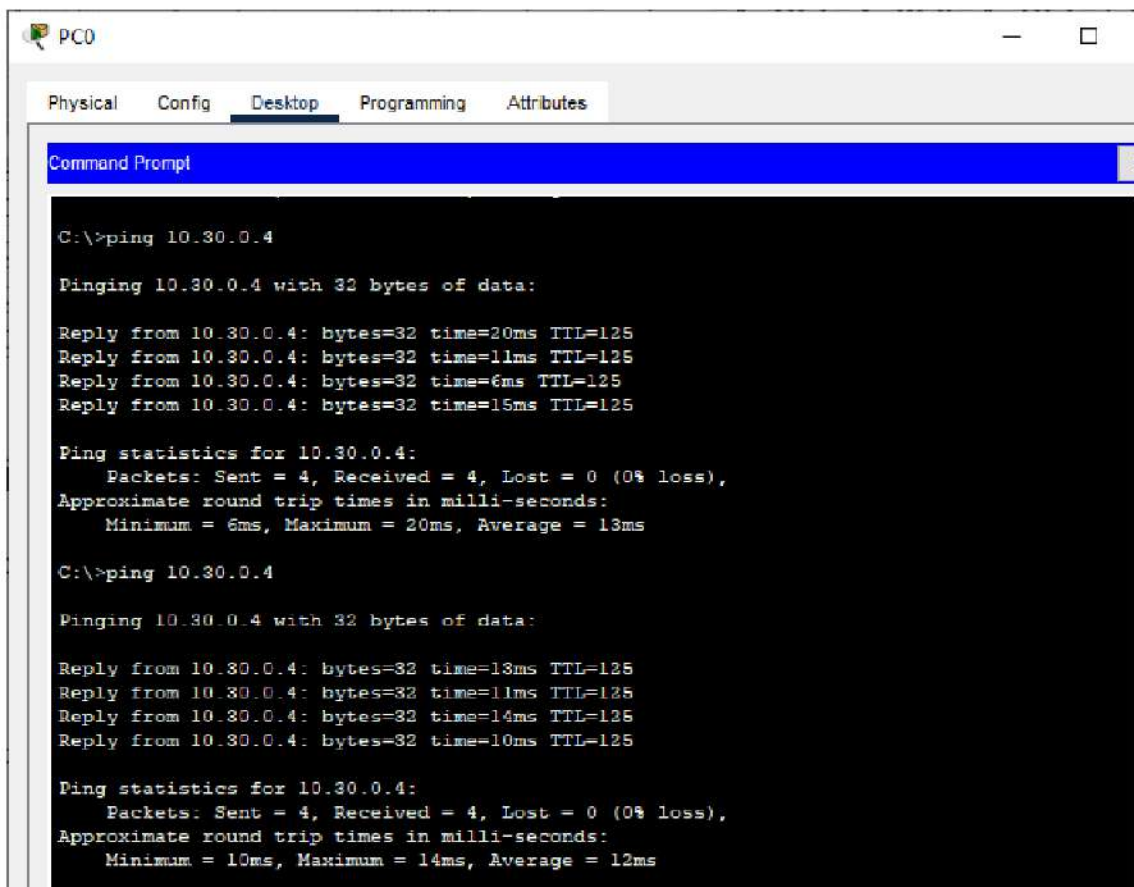
```

Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 10.30.0.0
Router(config-router)#network 192.168.1.0
Router(config-router)#exit
Router(config)#

```

Checking the connectivity by using the ping command

- i) Pinging PC8 (ip address 10.30.0.4) from PC0



The screenshot shows a PC0 desktop environment with a taskbar at the top containing icons for Physical, Config, Desktop, Programming, and Attributes. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The window has a blue title bar and a black background with white text. The text shows two successful ping operations to the IP address 10.30.0.4. Each operation consists of four replies and a summary of statistics. The first ping shows round trip times of 20ms, 11ms, 6ms, and 15ms, with an average of 13ms. The second ping shows round trip times of 13ms, 11ms, 14ms, and 10ms, with an average of 12ms. In both cases, all four packets were received with 0% loss.

```

C:\>ping 10.30.0.4

Pinging 10.30.0.4 with 32 bytes of data:

Reply from 10.30.0.4: bytes=32 time=20ms TTL=125
Reply from 10.30.0.4: bytes=32 time=11ms TTL=125
Reply from 10.30.0.4: bytes=32 time=6ms TTL=125
Reply from 10.30.0.4: bytes=32 time=15ms TTL=125

Ping statistics for 10.30.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 20ms, Average = 13ms

C:\>ping 10.30.0.4

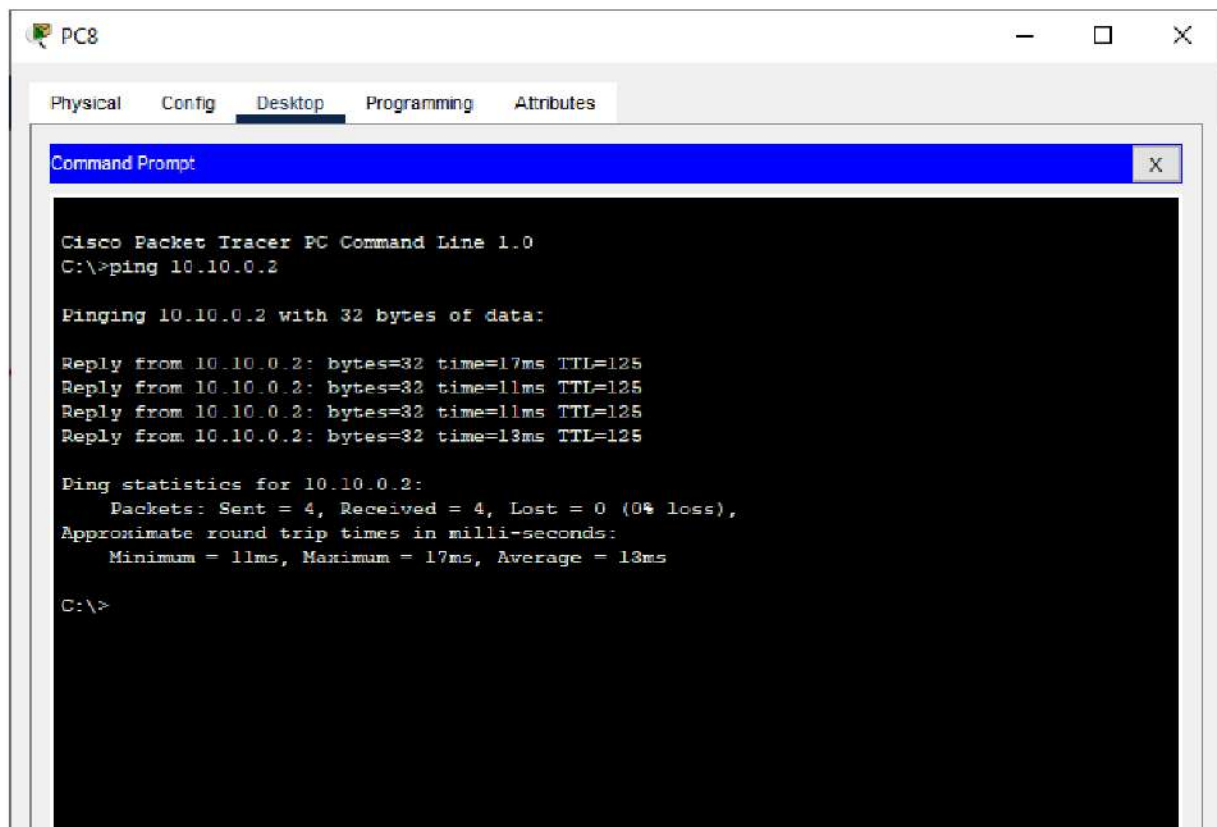
Pinging 10.30.0.4 with 32 bytes of data:

Reply from 10.30.0.4: bytes=32 time=13ms TTL=125
Reply from 10.30.0.4: bytes=32 time=11ms TTL=125
Reply from 10.30.0.4: bytes=32 time=14ms TTL=125
Reply from 10.30.0.4: bytes=32 time=10ms TTL=125

Ping statistics for 10.30.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 14ms, Average = 12ms

```


ii) Pinging PC0 (ip address 10.10.0.2) from PC8



The screenshot shows a Cisco Packet Tracer PC Command Line window for PC8. The window has tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, showing a Command Prompt window. The Command Prompt displays the output of the command 'ping 10.10.0.2'. The output shows four successful replies from 10.10.0.2 with varying times and TTL values. The ping statistics show 4 packets sent, 4 received, and 0% loss.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.0.2

Pinging 10.10.0.2 with 32 bytes of data:

Reply from 10.10.0.2: bytes=32 time=17ms TTL=125
Reply from 10.10.0.2: bytes=32 time=11ms TTL=125
Reply from 10.10.0.2: bytes=32 time=11ms TTL=125
Reply from 10.10.0.2: bytes=32 time=13ms TTL=125

Ping statistics for 10.10.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 17ms, Average = 13ms

C:\>
```

Result:

Hence the RIPv2 has been studied and verified through the given network

Click on the link or scan the QR-code for the video demonstration of the practical:

<https://youtu.be/qrBpjaxSkZY8>



Practical No 7

Aim: Using Packet Tracer, create a network with three routers with OSPF and each router associated network will have minimum three PC and show Connectivity

Theory:

Open shortest path first (OSPF) is a link-state routing protocol that is used to find the best path between the source and the destination router using its own shortest path first (SPF) algorithm. A link-state routing protocol is a protocol that uses the concept of triggered updates, i.e., if there is a change observed in the learned routing table then the updates are triggered only, not like the distance-vector routing protocol where the routing table is exchanged at a period of time.

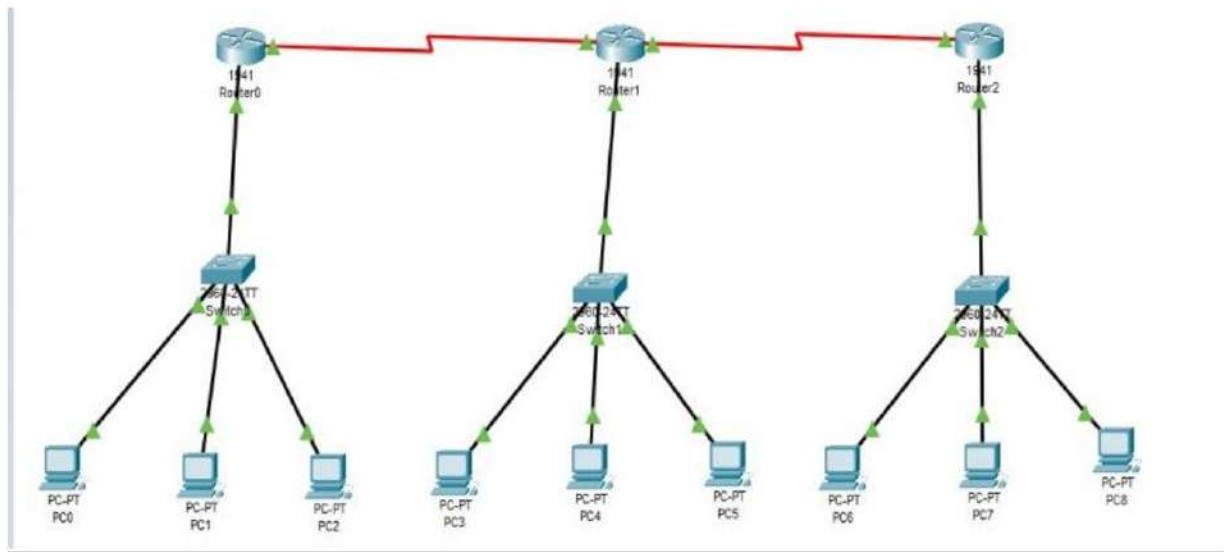
Open shortest path first (OSPF) is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e., the protocol which aims at moving the packet within a large autonomous system or routing domain.

OSPF advantages –

1. Both IPv4 and IPv6 routed protocols
2. Load balancing with equal-cost routes for the same destination
3. Unlimited hop counts
4. Trigger updates for fast convergence
5. A loop-free topology using SPF algorithm
6. Run on most routers
7. Classless protocol

There are some disadvantages of OSPF like, it requires an extra CPU process to run the SPF algorithm, requiring more RAM to store adjacency topology, and being more complex to set up and hard to troubleshoot.

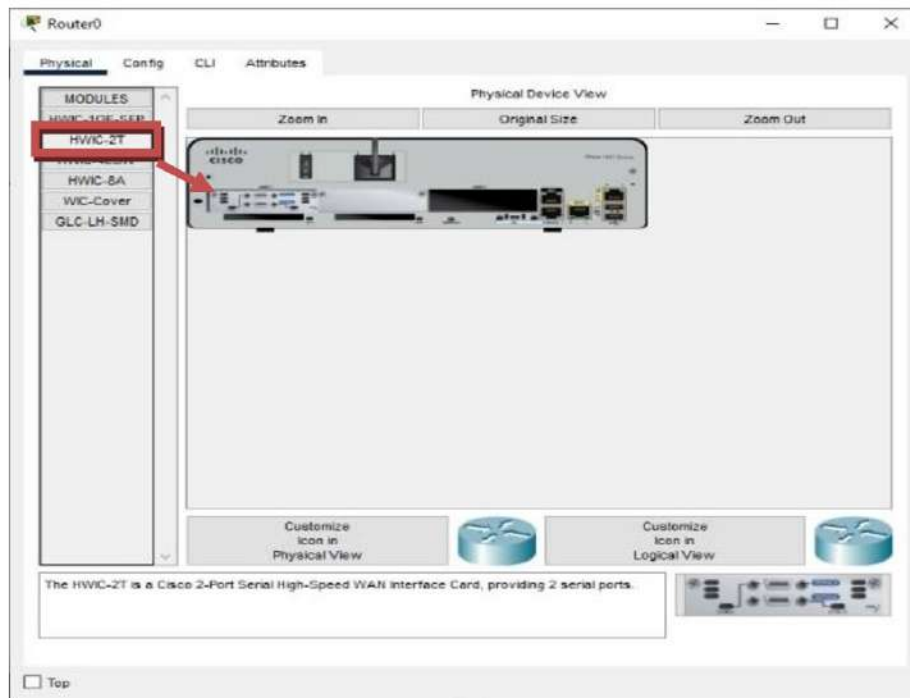
We use the following topology for the present case



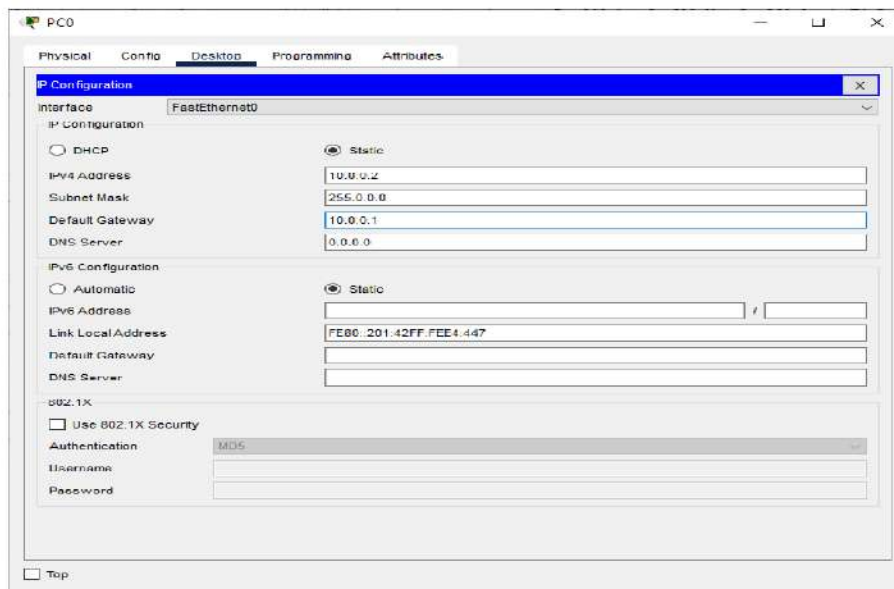
We configure the above network using the following IP addresses

Host	Interface	IP address	Default Gateway	Subnet Mask	Wildcard Mask
Router 0	G0/0	10.0.0.1		255.0.0.0	0.255.255.255
	S0/1/0	40.0.0.1			
Router 1	G0/0	20.0.0.1			
	S0/1/0	40.0.0.2			
	S0/1/1	50.0.0.1			
Router 2	G0/0	30.0.0.1			
	S0/1/1	50.0.0.2	10.0.0.1		
PC0	FastEthernet0	10.0.0.2			
PC1	FastEthernet0	10.0.0.3			
PC2	FastEthernet0	10.0.0.4	20.0.0.1		
PC3	FastEthernet0	20.0.0.2			
PC4	FastEthernet0	20.0.0.3			
PC5	FastEthernet0	20.0.0.4	30.0.0.1		
PC6	FastEthernet0	30.0.0.2			
PC7	FastEthernet0	30.0.0.3			
PC8	FastEthernet0	30.0.0.4			

Adding Serial Interface in each Router



Configuring PC0:



Configuring PC1:

PC1

Physical Config Desktop Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 10.0.0.3

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::205:5EFF:FE88:E00C

Default Gateway: /

DNS Server: /

802.1X

☐ Use 802.1X Security

Authentication: MDS

Username: /

Password: /

☐ Top

PC2

Physical Config Desktop Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static This address is already used in the network.

IPv4 Address: 10.0.0.4

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::2D0:BAFF:FE8E:684C

Default Gateway: /

DNS Server: /

802.1X

☐ Use 802.1X Security

Authentication: MDS

Username: /

Password: /

☐ Top

Configuring PC2:

PC2

Physical Config Desktop Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 20.0.0.2

Subnet Mask: 255.0.0.0

Default Gateway: 20.0.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::202:17FF:FE81:A06

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top

Configuring PC4:

PC4

Physical Config Desktop Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 20.0.0.3

Subnet Mask: 255.0.0.0

Default Gateway: 20.0.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::20A:41FF:FE13:AB7E

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top

PC5

Physical Config Desktop Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 20.0.0.4

Subnet Mask: 255.0.0.0

Default Gateway: 20.0.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::2E0:F9FF:FE0D:3AA

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top

Configuring PC6:

PC6

Physical Config Desktop Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 30.0.0.2

Subnet Mask: 255.0.0.0

Default Gateway: 30.0.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::2E0:F9FF:FE9A:D3AA

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top

Configuring PC7:

PC7

Physical Config Desktop Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 30.0.0.3

Subnet Mask: 255.0.0.0

Default Gateway: 30.0.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::201:C9FF:FECD:D846

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top

Configuring PC8:

PC8

Physical Config Desktop Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 30.0.0.4

Subnet Mask: 255.0.0.0

Default Gateway: 30.0.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::280:3EFF:FE25:E1BE

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

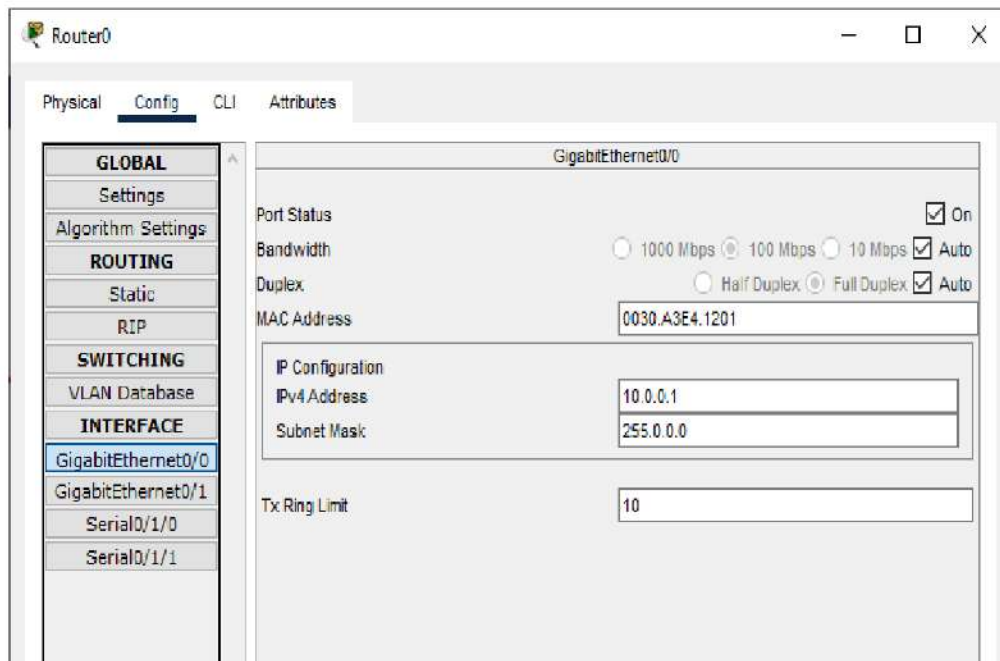
Username:

Password:

☐ Top

Configuring IP addresses on Router 0

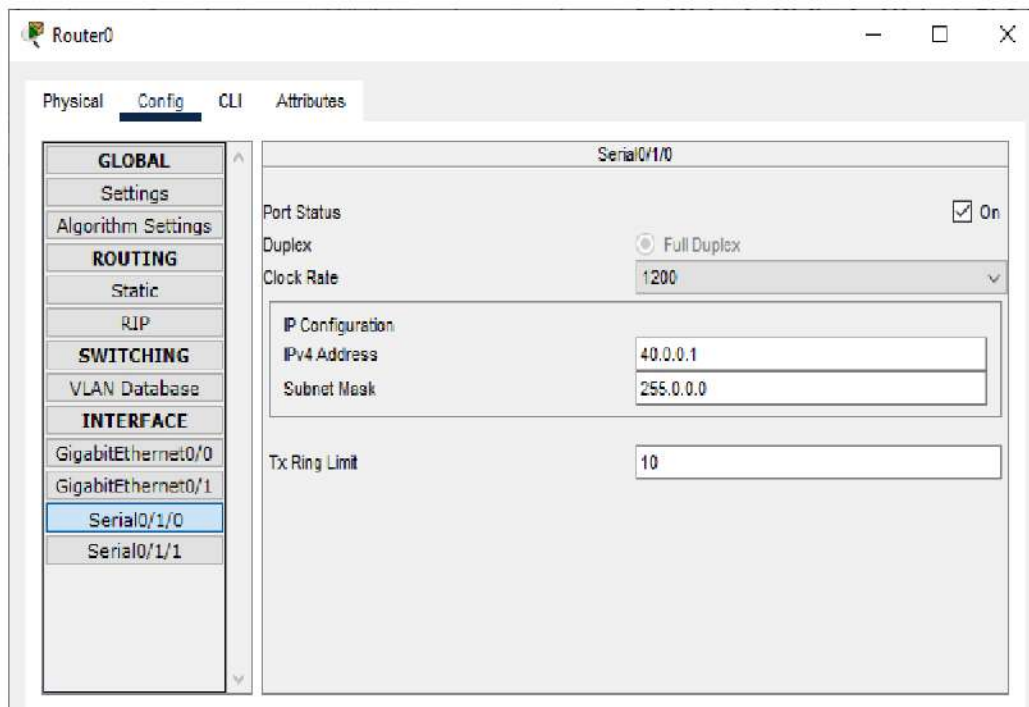
i) Interface G0/0



The screenshot shows the configuration window for Router0, specifically the 'Config' tab for the GigabitEthernet0/0 interface. The left sidebar shows a tree view with categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under INTERFACE, GigabitEthernet0/0 is selected. The main configuration area for GigabitEthernet0/0 includes:

- Port Status:** ☒ On
- Bandwidth:** Radio buttons for 1000 Mbps, 100 Mbps (selected), and 10 Mbps. ☒ Auto
- Duplex:** Radio buttons for Half Duplex and Full Duplex (selected). ☒ Auto
- MAC Address:** 0030.A3E4.1201
- IP Configuration:**
 - IPv4 Address:** 10.0.0.1
 - Subnet Mask:** 255.0.0.0
- Tx Ring Limit:** 10

ii) Interface S0/1/0

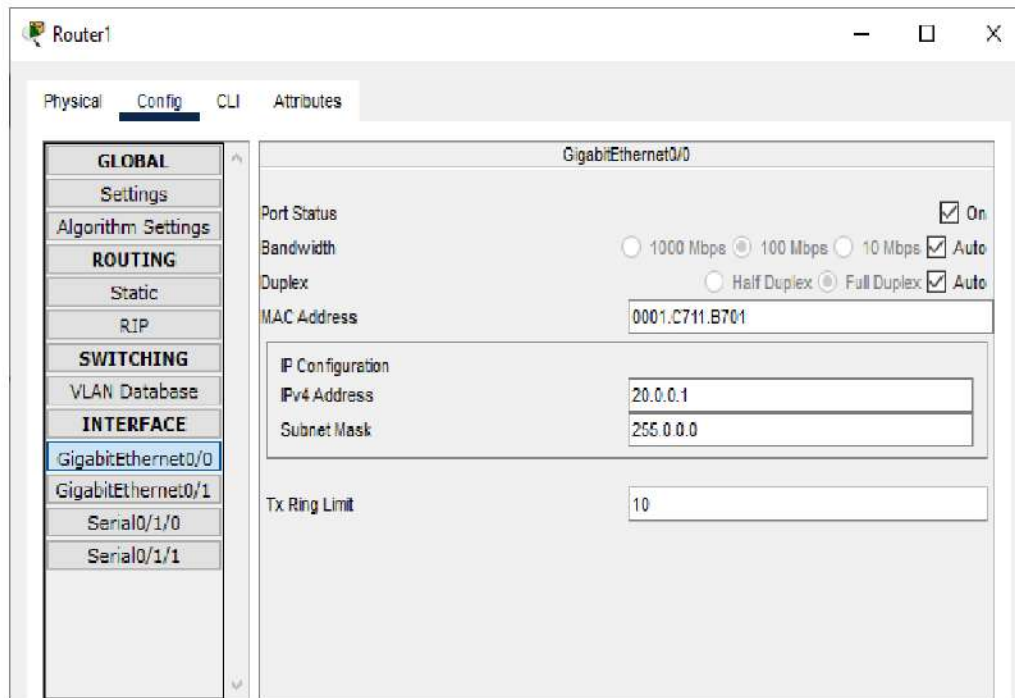


The screenshot shows the configuration window for Router0, specifically the 'Config' tab for the Serial0/1/0 interface. The left sidebar shows a tree view with categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under INTERFACE, Serial0/1/0 is selected. The main configuration area for Serial0/1/0 includes:

- Port Status:** ☒ On
- Duplex:** ☒ Full Duplex
- Clock Rate:** 1200
- IP Configuration:**
 - IPv4 Address:** 40.0.0.1
 - Subnet Mask:** 255.0.0.0
- Tx Ring Limit:** 10

Configuring IP addresses on Router 1

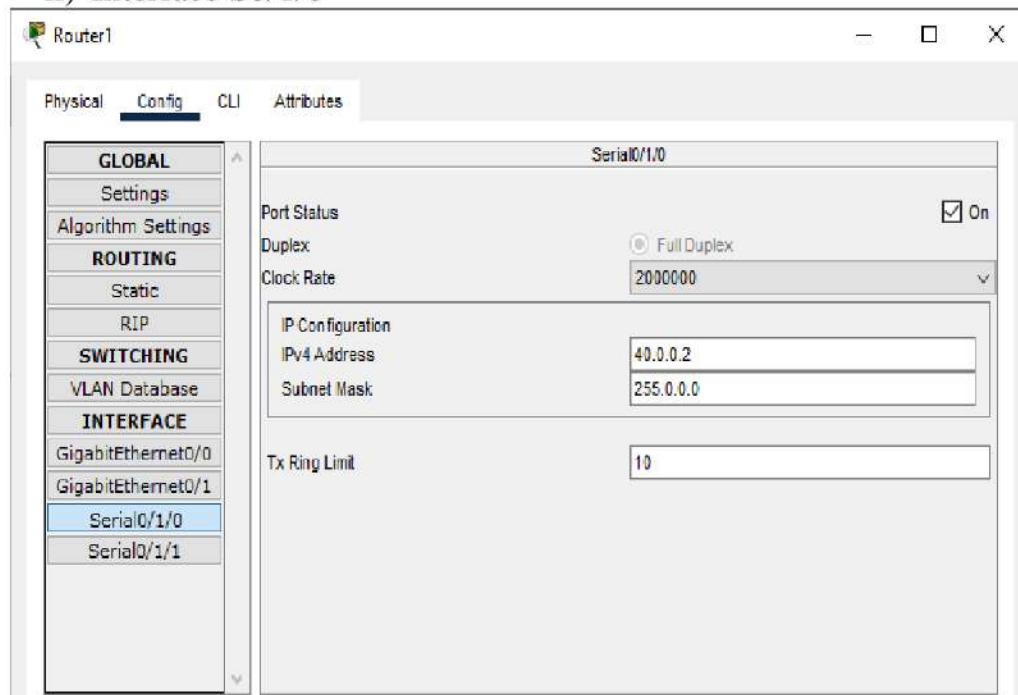
i) Interface G0/0



The screenshot shows the configuration window for Router1, specifically the 'Config' tab for the GigabitEthernet0/0 interface. The left sidebar shows a tree view with categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under INTERFACE, GigabitEthernet0/0 is selected. The main configuration area for GigabitEthernet0/0 includes the following settings:

- Port Status:** ☒ On
- Bandwidth:** ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto
- Duplex:** ☐ Half Duplex ☒ Full Duplex ☒ Auto
- MAC Address:** 0001.C711.B701
- IP Configuration:**
 - IPv4 Address:** 20.0.0.1
 - Subnet Mask:** 255.0.0.0
- Tx Ring Limit:** 10

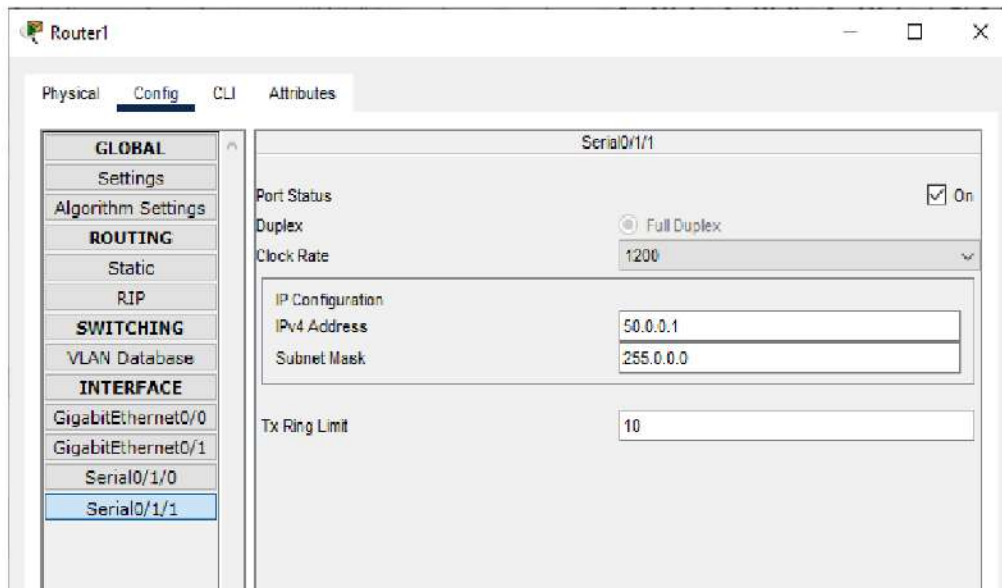
ii) Interface S0/1/0



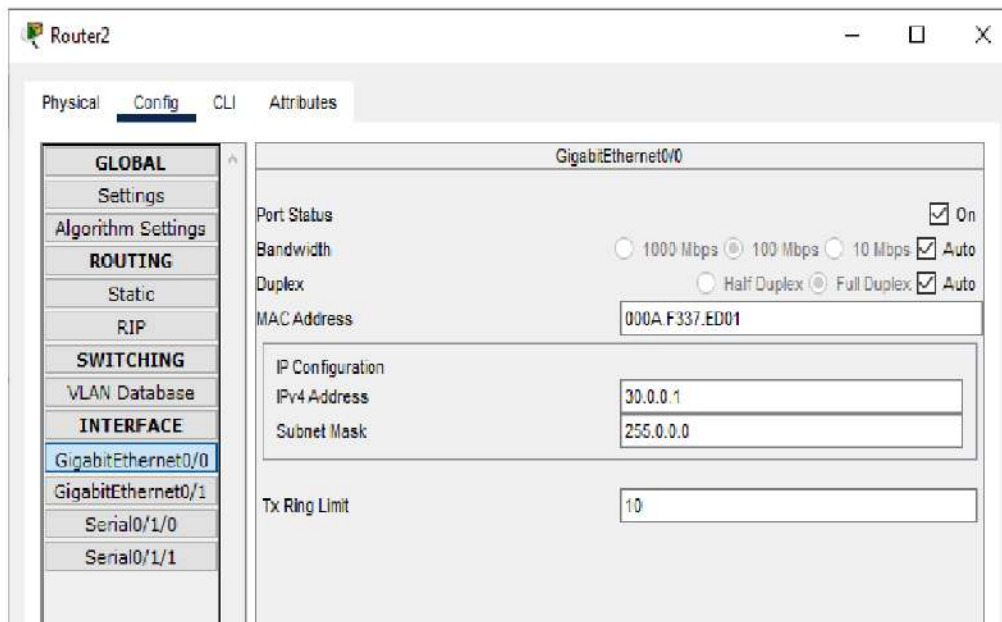
The screenshot shows the configuration window for Router1, specifically the 'Config' tab for the Serial0/1/0 interface. The left sidebar shows a tree view with categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under INTERFACE, Serial0/1/0 is selected. The main configuration area for Serial0/1/0 includes the following settings:

- Port Status:** ☒ On
- Duplex:** ☒ Full Duplex
- Clock Rate:** 2000000
- IP Configuration:**
 - IPv4 Address:** 40.0.0.2
 - Subnet Mask:** 255.0.0.0
- Tx Ring Limit:** 10

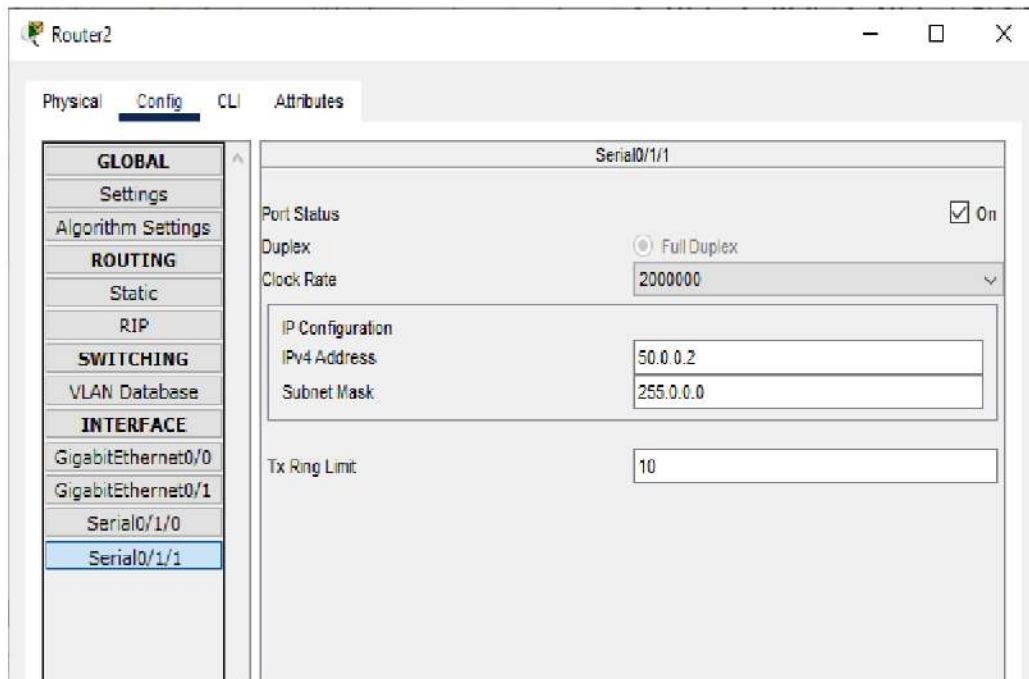
iii) Interface S0/1/1

**Configuring IP addresses on Router 2**

i) Interface G0/0



ii) Interface S0/1/1

**Configuring Router 0 for OSPF (using the CLI mode)**

```
Router(config)#
Router(config)#router ospf 1
Router(config-router)#network 10.0.0.0 0.0.0.255 area 1
Router(config-router)#network 40.0.0.0 0.0.0.255 area 1
Router(config-router)#exit
Router(config)#
```

Configuring Router 1 for OSPF (using the CLI mode)

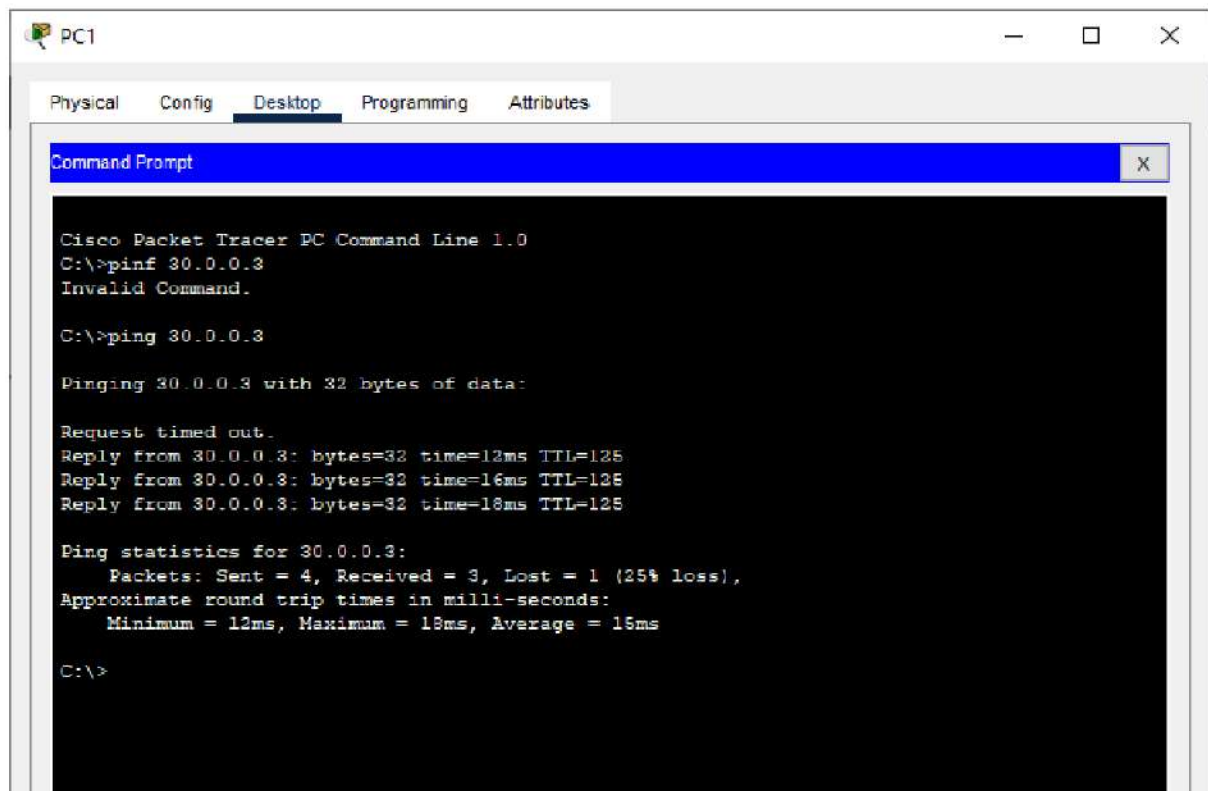
```
Router(config)#
Router(config)#router ospf 1
Router(config-router)#
Router(config-router)#network 20.0.0.0 0.0.0.255 area 1
Router(config-router)#network 40.0.0.0 0.0.0.255 area 1
Router(config-router)#network 50.0.0.0 0.0.0.255 area 1
Router(config-router)#exit
Router(config)#
```


Configuring Router 2 for OSPF (using the CLI mode)

```
Router(config)#  
Router(config)#router ospf 1  
Router(config-router)#  
Router(config-router)#network 30.0.0.0 0.0.0.255 area 1  
Router(config-router)#network 50.0.0.0 0.0.0.255 area 1  
Router(config-router)# exit  
Router(config)#
```

Checking the connectivity by using the ping command

- i) Pinging PC8 (ip address 10.30.0.4) from PC1



ii) Pinging PC0 (ip address 10.10.0.2) from PC8

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Request timed out.
Reply from 10.0.0.2: bytes=32 time=12ms TTL=125
Reply from 10.0.0.2: bytes=32 time=15ms TTL=125
Reply from 10.0.0.2: bytes=32 time=13ms TTL=125

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 15ms, Average = 13ms

C:\>

```

Result:

Hence the OSPF has been studied and verified through the given network

Click on the link or scan the QR-code for the video demonstration of the practical:

<https://youtu.be/PVaQ3M-Jiq8>



Practical No 8

Aim: Using Packet Tracer, create a network with three routers with BGP and each router associated network will have minimum three PC and show Connectivity

Theory:

Border Gateway Protocol (BGP) is used to Exchange routing information for the internet and is the protocol used between ISP which are different Autonomous Systems (AS).

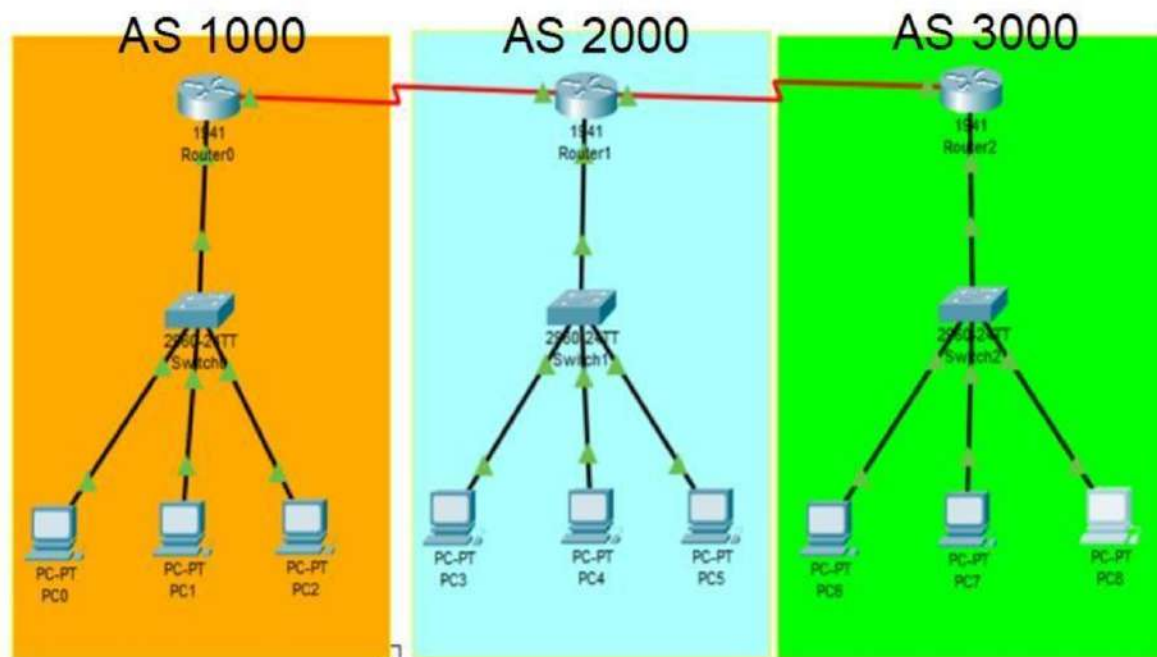
The protocol can connect together any internetwork of autonomous system using an arbitrary topology. The only requirement is that each AS have at least one router that is able to run BGP and that is router connect to at least one other AS's BGP router.

BGP's main function is to exchange network reach-ability information with other BGP systems.

Characteristics of Border Gateway Protocol (BGP):

- a) The main role of BGP is to provide communication between two autonomous systems.
- b) BGP supports Next-Hop Paradigm.
- c) Coordination among multiple BGP speakers within the AS (Autonomous System).
- d) BGP advertisement also include path information, along with the reachable destination and next destination pair.
- e) BGP can implement policies that can be configured by the administrator.
- f) BGP runs Over TCP.
- g) BGP conserve network Bandwidth.
- h) BGP supports CIDR.
- i) BGP also supports Security

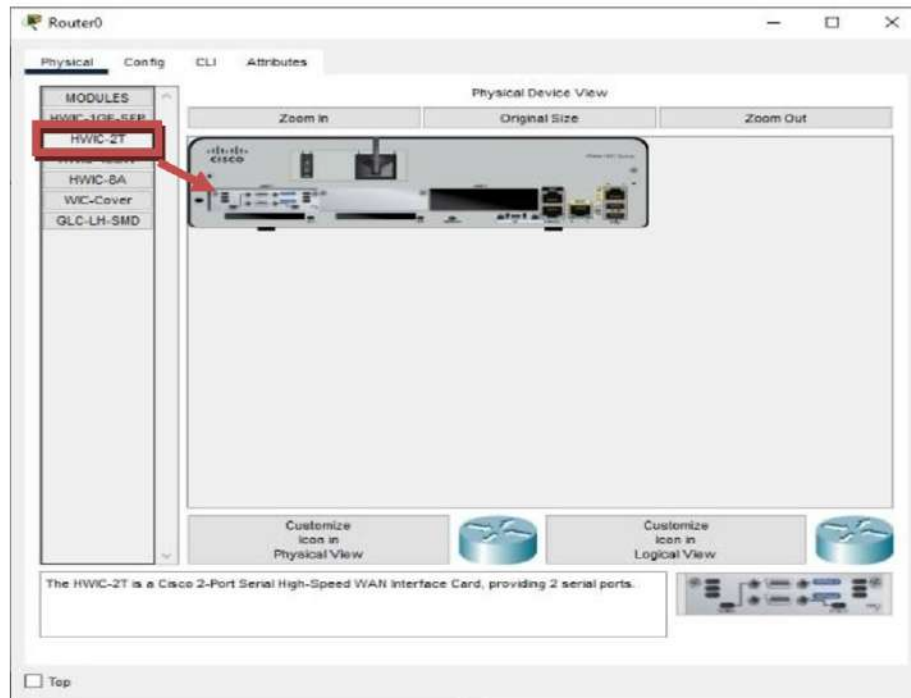
We use the following topology for the present case



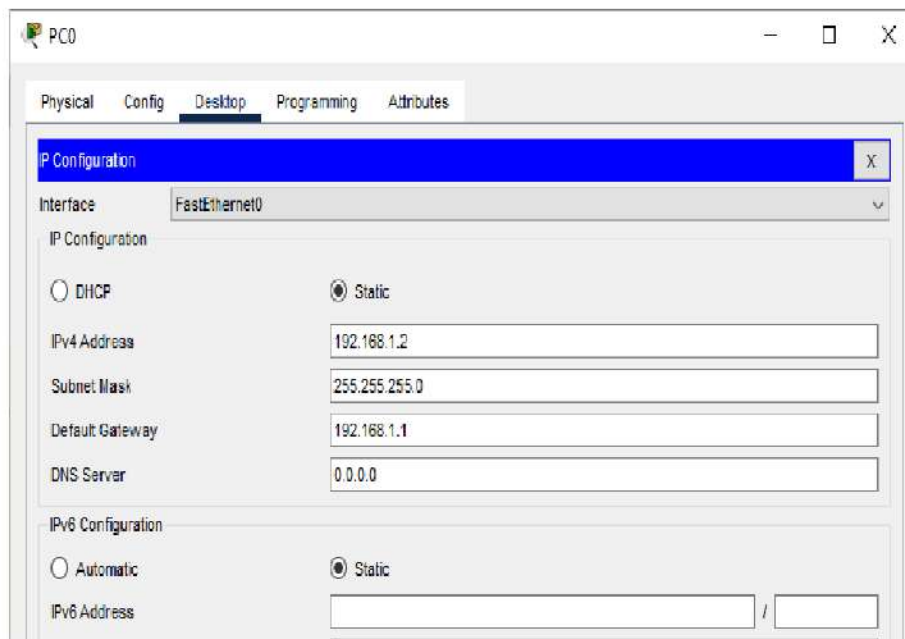
We configure the above network using the following IP addresses

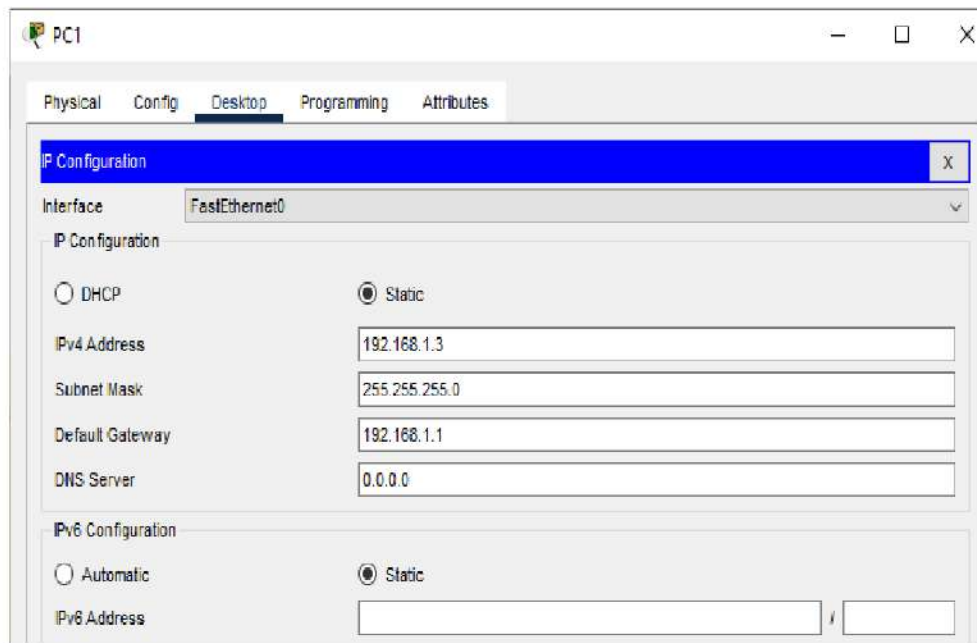
Host	Interface	IP address	Network Address	Default Gateway
Router 0 AS 1000	G0/0	192.168.1.1	192.168.1.0	
	S0/1/0	10.0.0.1	10.0.0.0	
Router 1 AS 2000	G0/0	192.168.2.1	192.168.2.0	
	S0/1/0	10.0.0.2	10.0.0.0	
	S0/1/1	20.0.0.1	20.0.0.0	
Router 2 AS 3000	G0/0	192.168.3.1	192.168.3.0	
	S0/1/1	20.0.0.2	20.0.0.0	
PC0	FastEthernet0	192.168.1.2	192.168.1.0	192.168.1.1
PC1	FastEthernet0	192.168.1.3		
PC2	FastEthernet0	192.168.1.4		
PC3	FastEthernet0	192.168.2.2	192.168.2.0	192.168.2.1
PC4	FastEthernet0	192.168.2.3		
PC5	FastEthernet0	192.168.2.4		
PC6	FastEthernet0	192.168.3.2	192.168.3.0	192.168.3.1
PC7	FastEthernet0	192.168.3.3		
PC8	FastEthernet0	192.168.3.4		

Adding Serial Interface in each Router

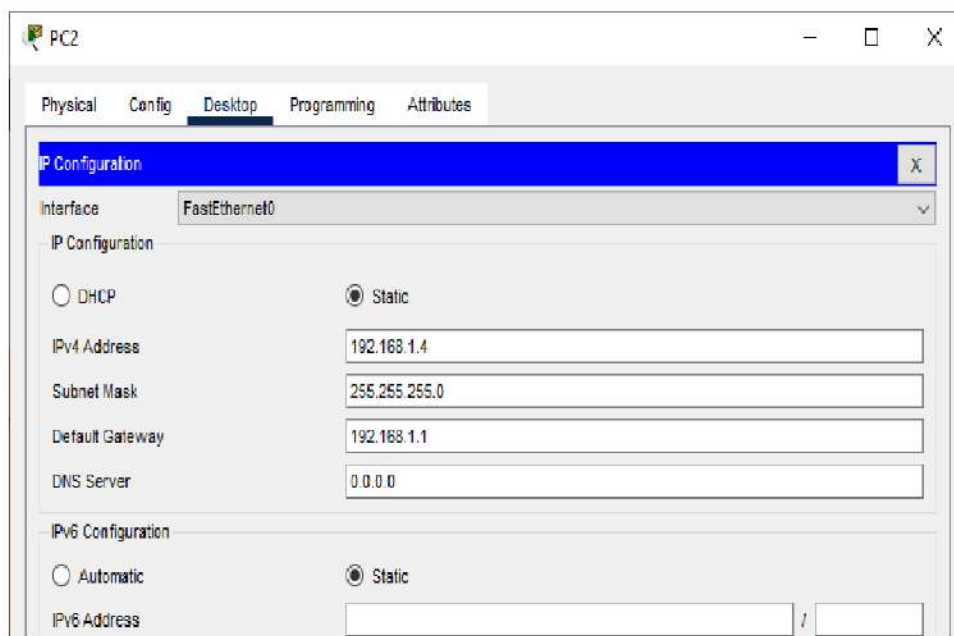


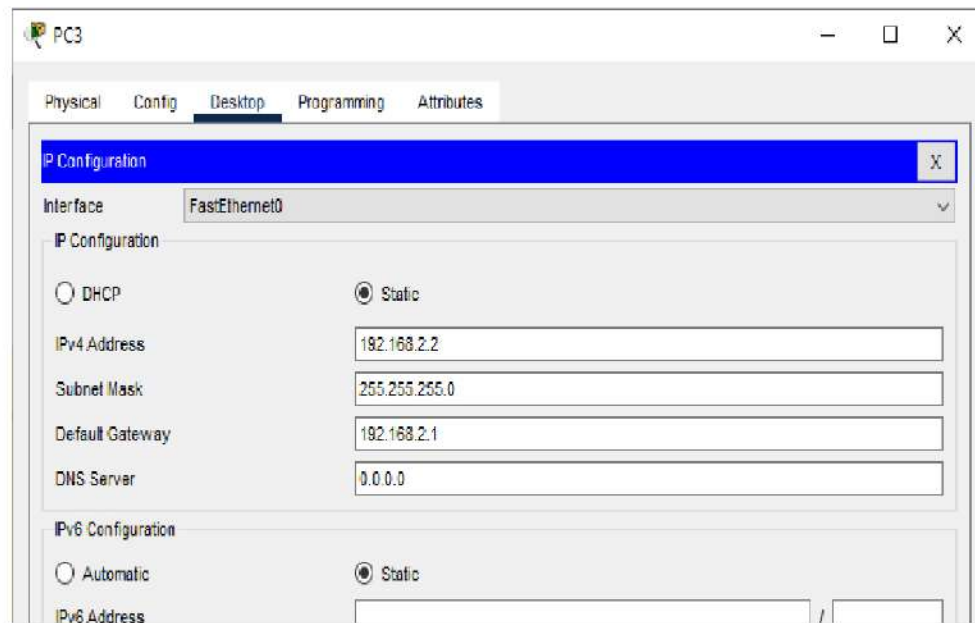
Configuring PC0:



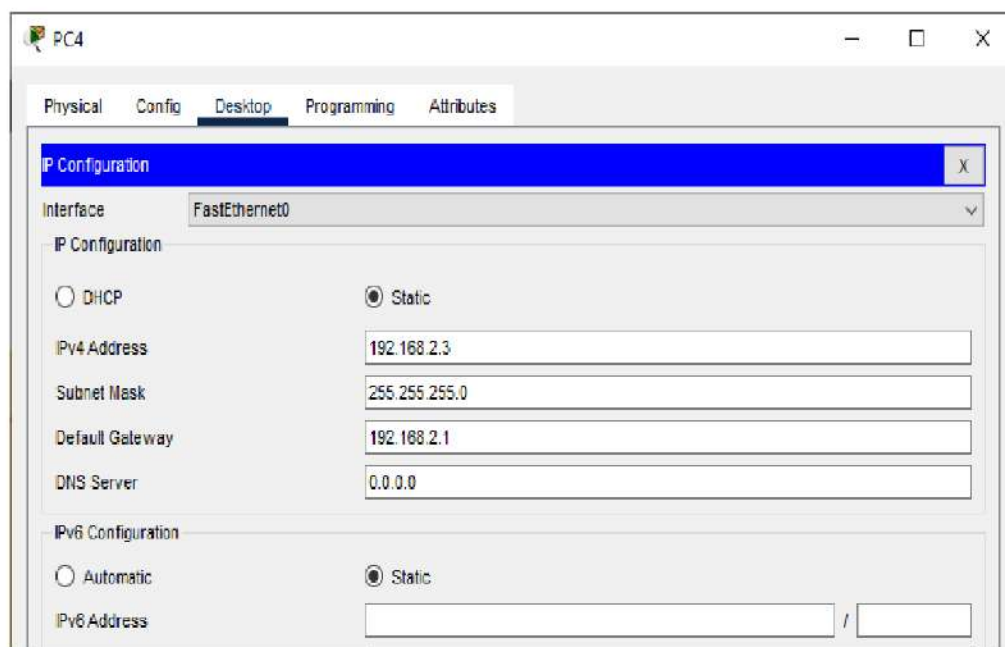


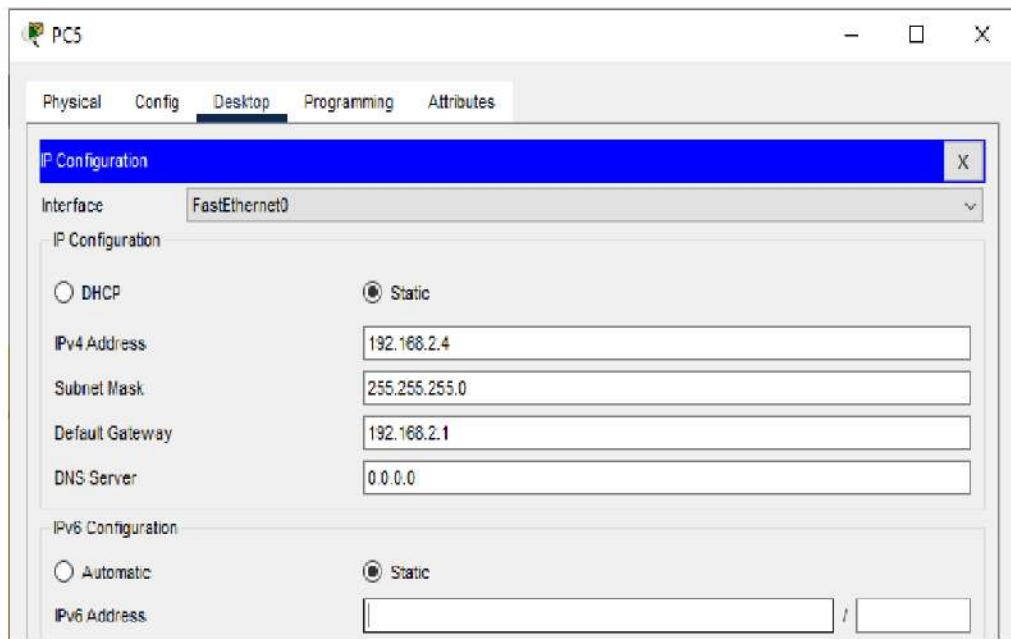
Configuring PC2:



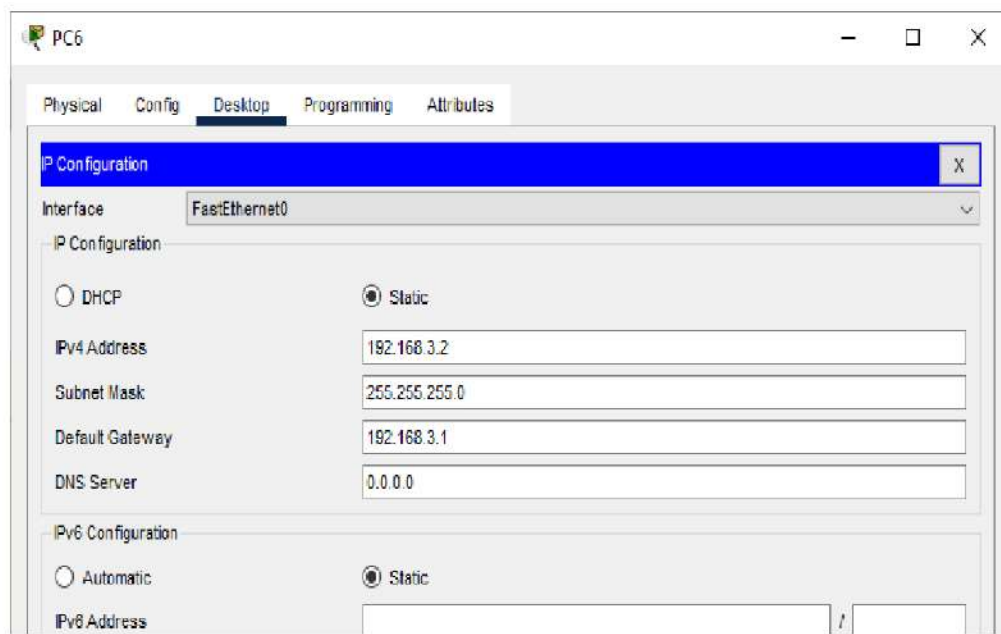


Configuring PC4:

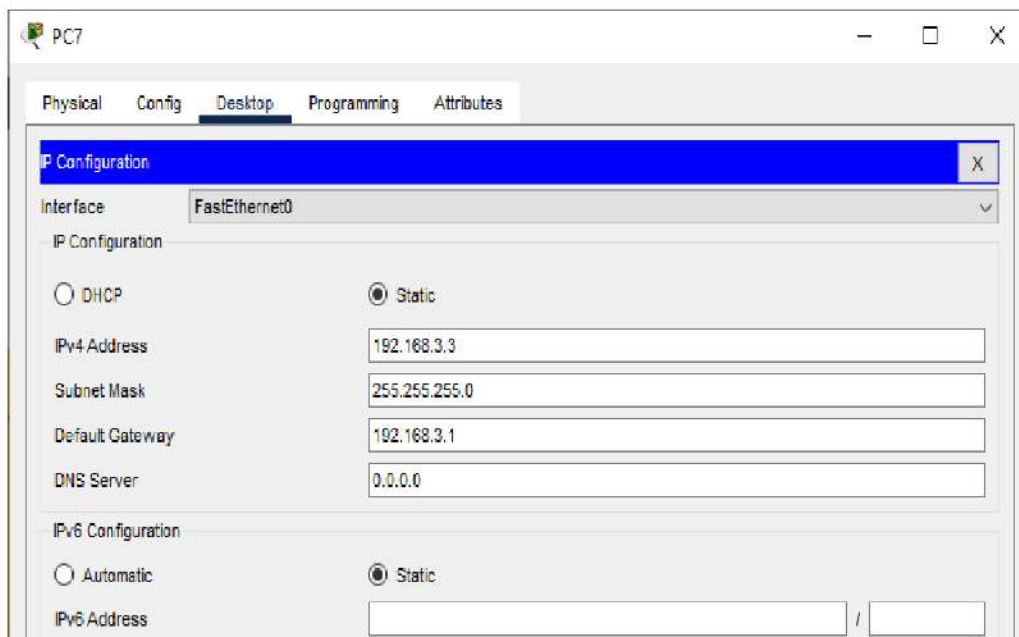




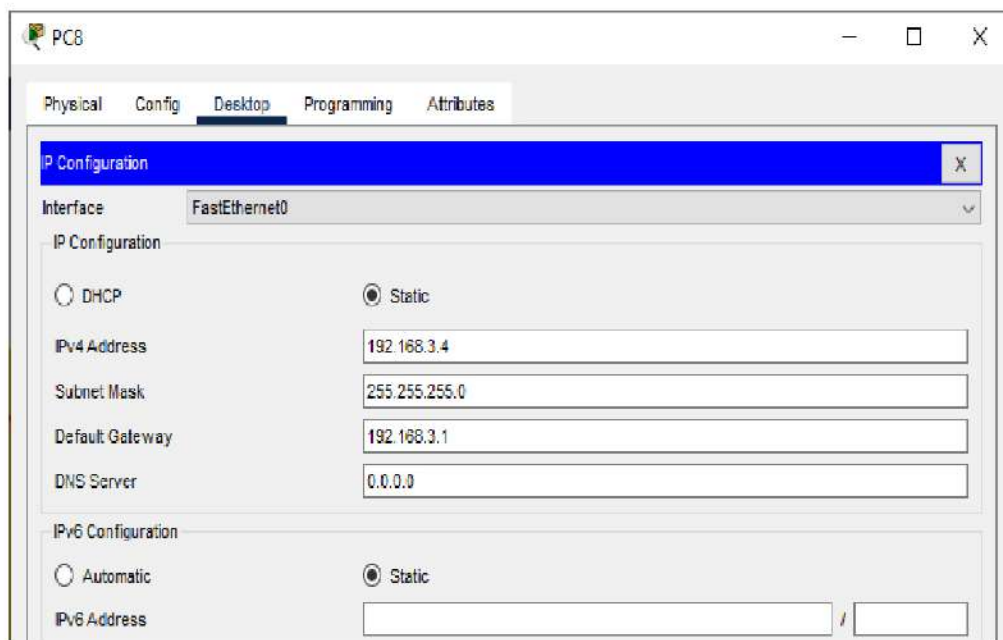
Configuring PC6:



Configuring PC7:

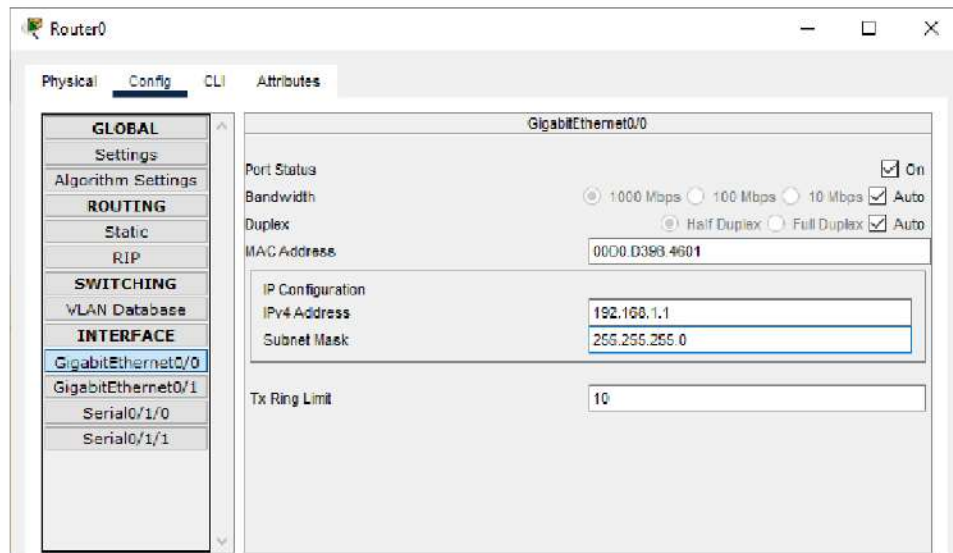


Configuring PC8:

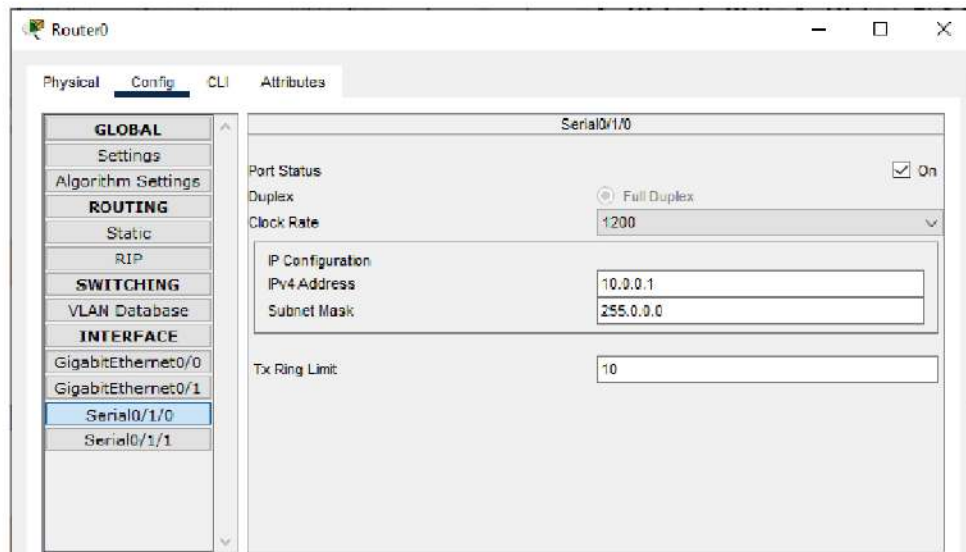


Configuring IP addresses on Router 0

i) Interface G0/0



ii) Interface S0/1/0



Practical No 10

Aim: Using Wire-shark to capture and analyze Packets

Theory:

Wireshark is popular and powerful network protocol analyzer software. It is primarily used for:

1. **Network Troubleshooting:** Wireshark allows you to capture and inspect network traffic in real-time or from previously captured packet data. This is invaluable for diagnosing and resolving network problems, such as connectivity issues, slow network performance, and packet loss. You can identify where packets are being dropped or delayed and pinpoint the source of network issues.
2. **Security Analysis:** Wireshark can be used to detect and investigate security breaches and malicious activity on a network. By examining network traffic, security professionals can identify suspicious or unauthorized activities, such as intrusion attempts, malware infections, and data exfiltration. It's an essential tool for network security monitoring.
3. **Network Protocol Analysis:** Wireshark supports a wide range of network protocols, and it allows you to analyze and decode packets to understand how different devices and applications communicate over the network. This is helpful for developers, network administrators, and security analysts who need to understand the behavior of network protocols and applications.
4. **Network Performance Optimization:** By analyzing network traffic patterns, Wireshark can help optimize network performance. You can identify bandwidth hogs, inefficient network configurations, and bottlenecks in the network infrastructure. This information can be used to fine-tune network settings and improve overall performance.
5. **Educational and Training Purposes:** Wireshark is often used in educational settings and for training purposes to teach networking concepts and packet analysis techniques. It provides a hands-on way to learn about network protocols and their interactions.
6. **Compliance and Auditing:** Some organizations use Wireshark for compliance and auditing purposes. It helps ensure that network traffic conforms to security policies and regulatory requirements. Organizations can use Wireshark to monitor and record network activities for auditing and legal purposes.
7. **Software Development:** Developers use Wireshark to debug network-related issues in their applications. It can help identify problems with network communication and assist in troubleshooting.
8. **Packet Capture and Analysis:** Wireshark allows you to capture packets from various network interfaces and save them for later analysis. You can filter and search through the captured data to extract specific information and gain insights into network behaviour.
9. **Prototyping and Testing:** Wireshark can be used to test and validate network configurations and prototypes before they are deployed in a production environment. It helps ensure that new network setups work as expected and meet performance criteria.

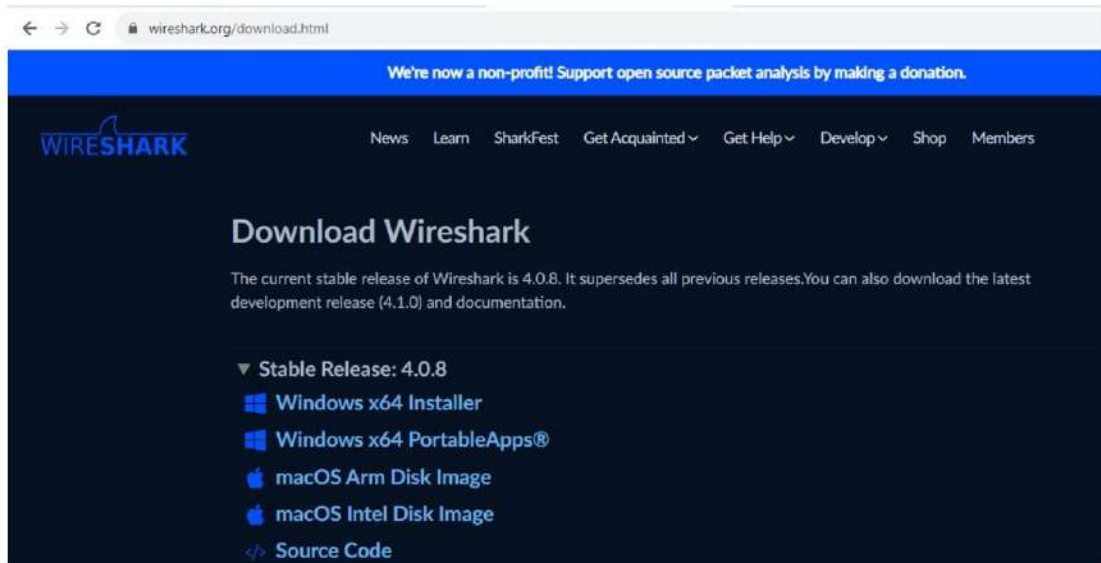
Wireshark's user-friendly interface, extensive protocol support, and robust filtering capabilities make it a

valuable tool for anyone involved in networking, security, or network-related development tasks. However, it's important to note that using Wireshark to capture and analyze network traffic may have legal and privacy considerations, so it should be used responsibly and in compliance with applicable laws and policies.

Install Wireshark:

In order to demonstrate the packet capture and analysis, we install Wireshark by visiting the website www.wireshark.org/download

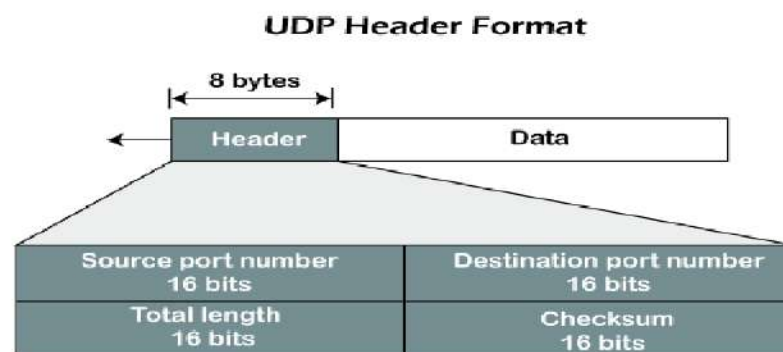
And download the software according to our OS



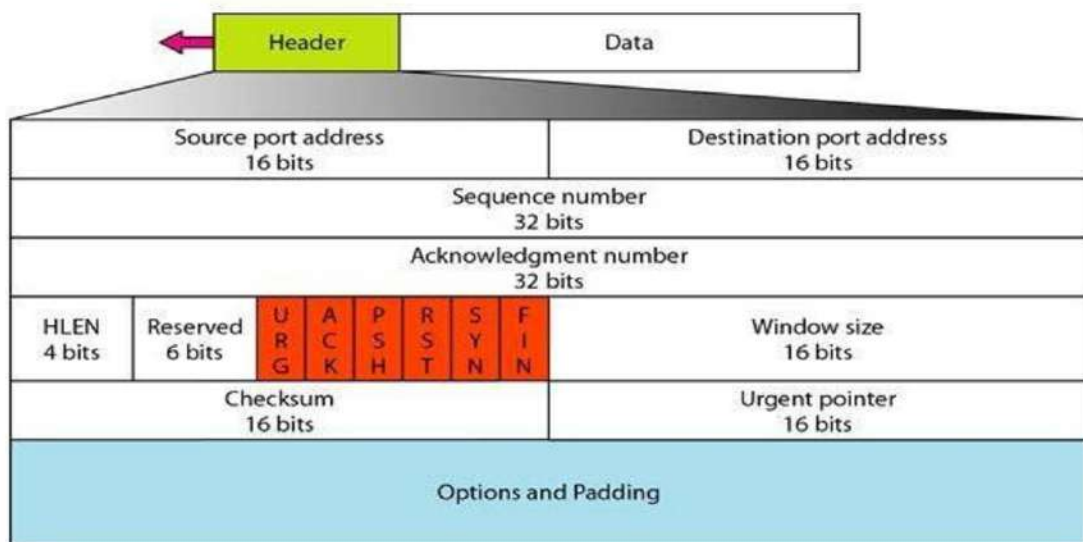
Analysis:

Before doing the analysis of the packets, we must first know the UDP, TCP and IP packet format

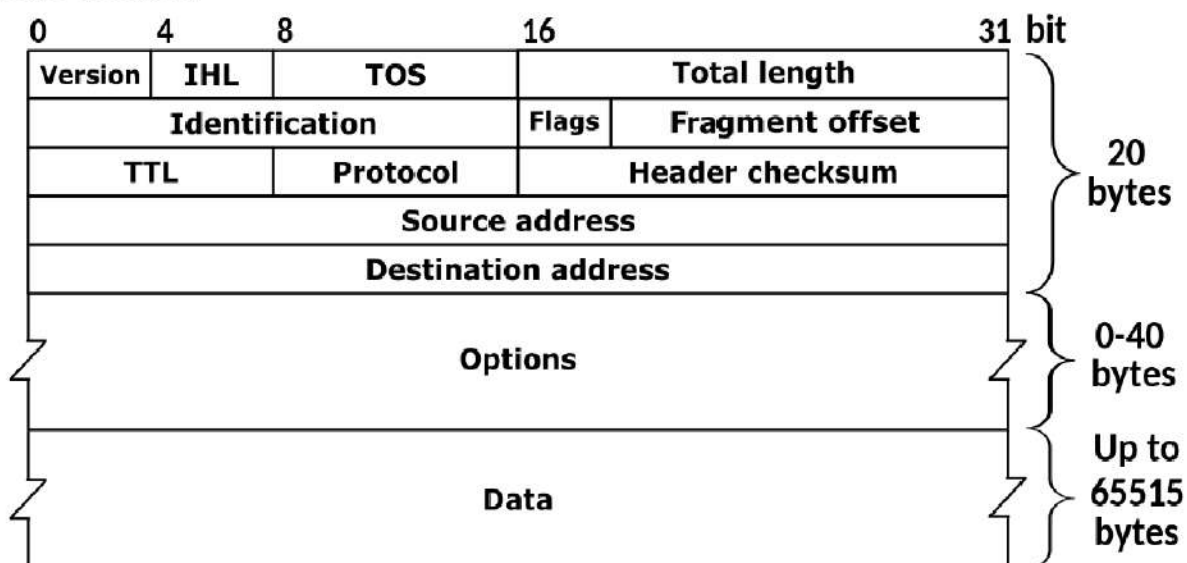
UDP Packet format



TCP Segment format:

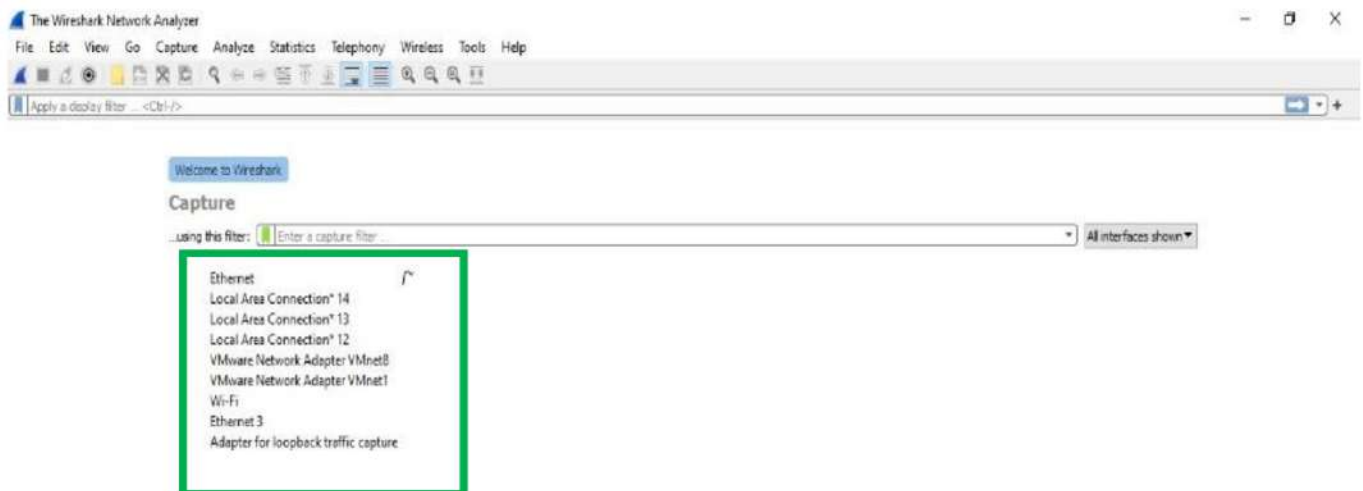


IP packet format:

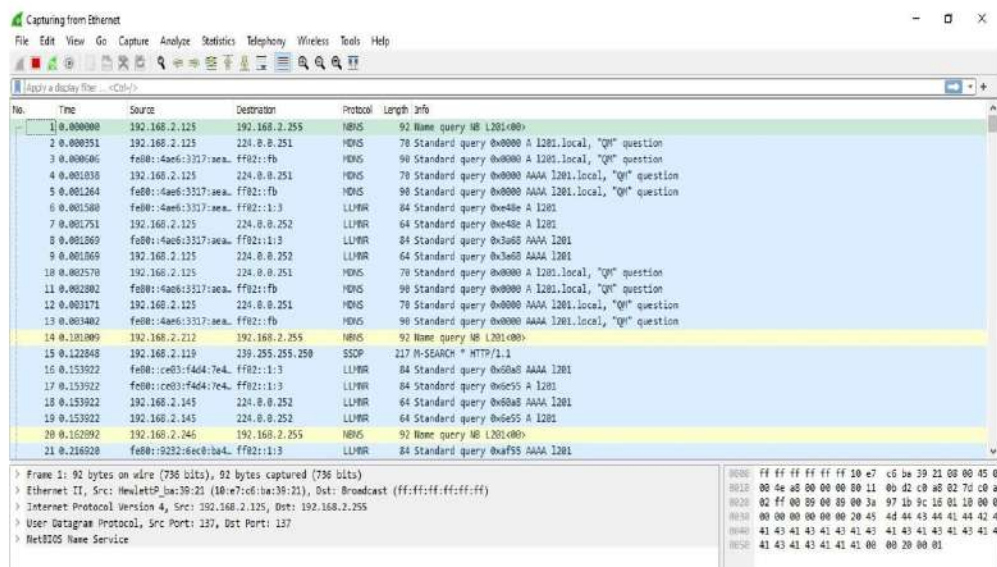


Using Wire-Shark:

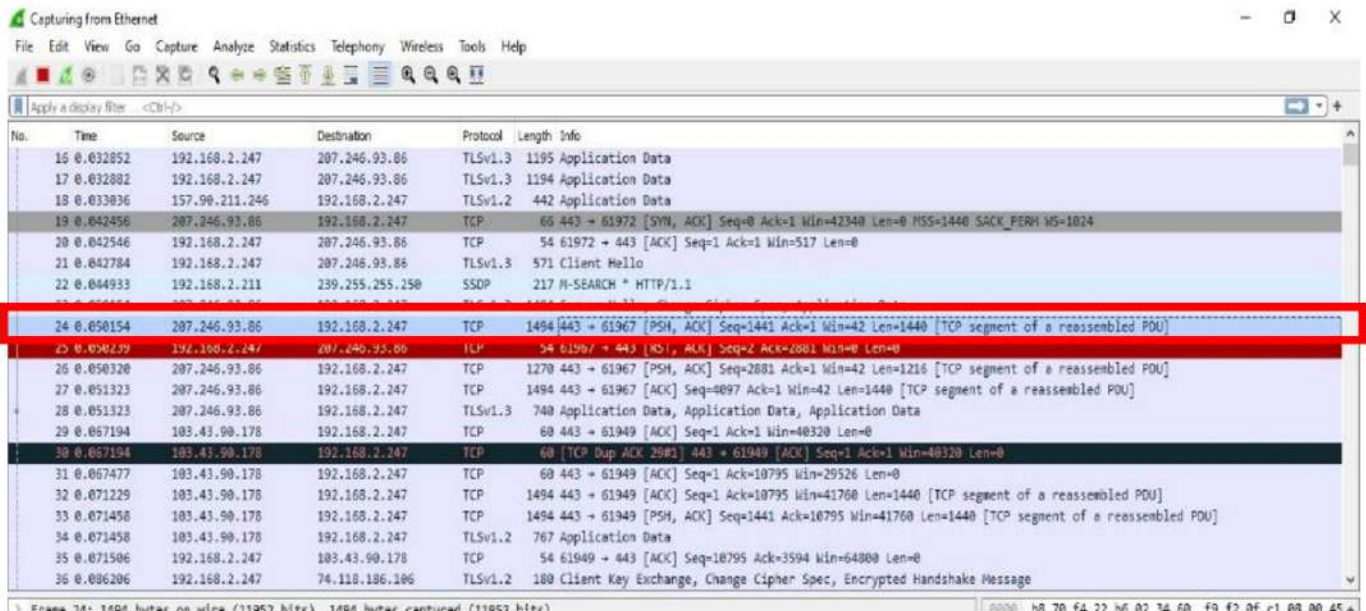
We use Wireshark to do the analysis of the packet, we get the following interface when we start Wireshark



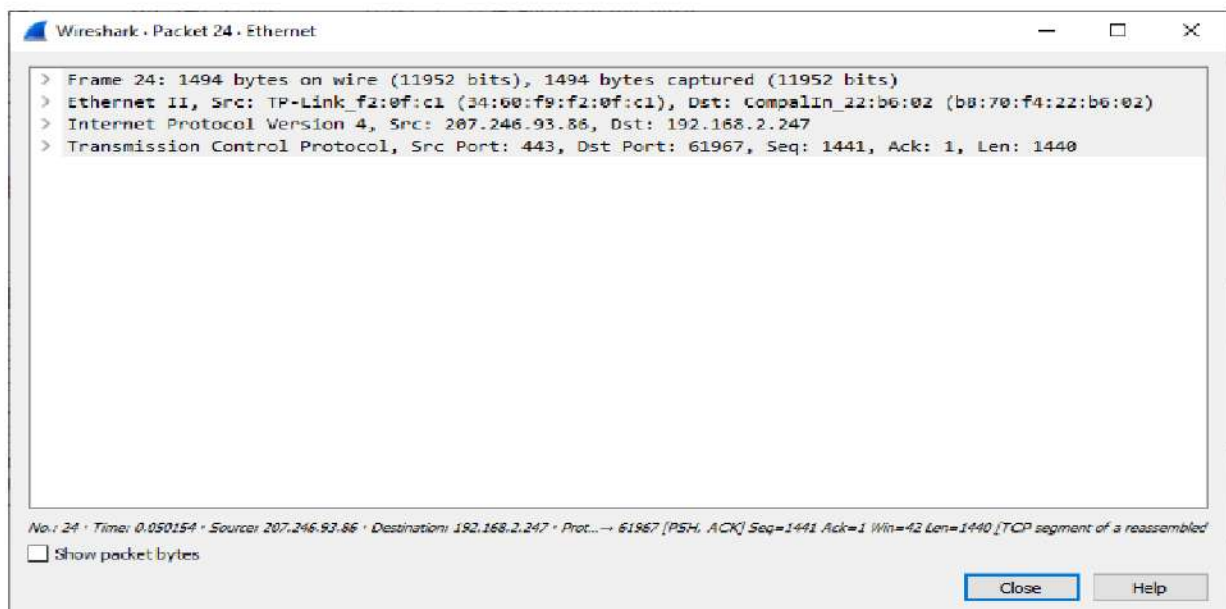
The above interfaces are shown, as in our case the internet connection is available on the Ethernet interface, we double click on this interface and get the following



Now we click on any TCP packet and analyze it,

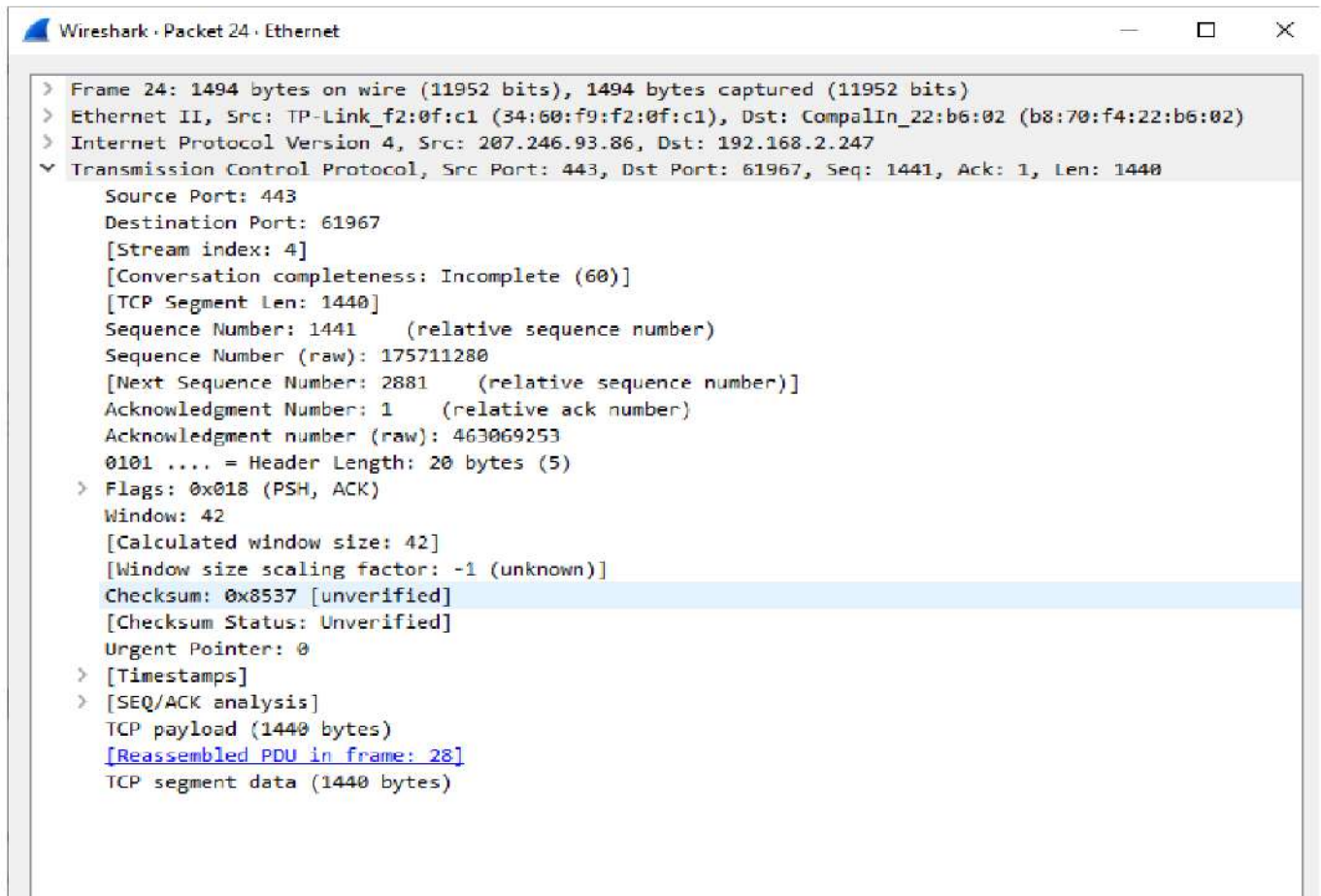


When we double click on the above TCP packet (packet 24) in the above case we get



TCP segment analysis:

When we click on Transmission Control Protocol (TCP), we get the information about the TCP segment and we can analyse the segment



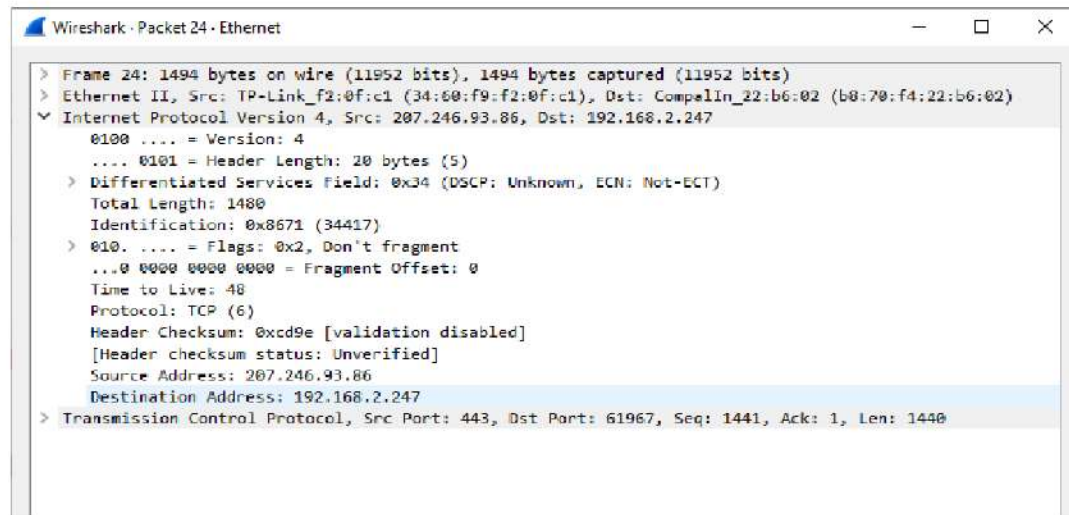
As seen from the above we get

Source Port: 443
 Destination Port: 61967
 Sequence number 1441
 Acknowledgement Number: 1

And also the other information such Flags, Window, Urgent Pointer etc

IP packet analysis:

When we click on Internet Protocol Version 4, we get the information about the IPv4 packet and we can analyse it



We can easily analyse the packet and get the information about the IP packet

Source IP address: 207.246.93.86

Destination IP address: 192.168.2.247 Header Length: 20 bytes

Total Length: 1480

Other fields are also seen

Similarly we can also analyse any UDP packet

For the video demonstration of the practical click on the link below or scan the QR-code

<https://youtu.be/pT93ag0zSXQ>



Configuring IP addresses on Router 1

i) Interface G0/0

The screenshot shows the configuration window for Router1, specifically for the GigabitEthernet0/0 interface. The window has tabs for Physical, Config, CLI, and Attributes. The Config tab is active. On the left, there is a tree view with categories: GLOBAL, Settings, Algorithm Settings, ROUTING, Static, RIP, SWITCHING, VLAN Database, and INTERFACE. Under the INTERFACE category, GigabitEthernet0/0 is selected. The main area displays the configuration for GigabitEthernet0/0. It includes fields for Port Status (checked On), Bandwidth (1000 Mbps selected, Auto checked), Duplex (Half Duplex selected, Full Duplex checked, Auto checked), MAC Address (0090.2B5B.9E01), IP Configuration (IPv4 Address: 192.168.2.1, Subnet Mask: 255.255.255.0), and Tx Ring Limit (10).

GigabitEthernet0/0	
Port Status	☒ On
Bandwidth	☒ 1000 Mbps ☐ 100 Mbps ☐ 10 Mbps ☒ Auto
Duplex	☒ Half Duplex ☐ Full Duplex ☒ Auto
MAC Address	0090.2B5B.9E01
IP Configuration	
IPv4 Address	192.168.2.1
Subnet Mask	255.255.255.0
Tx Ring Limit	10

ii) Interface S0/1/0

The screenshot shows the configuration window for Router1, specifically for the Serial0/1/0 interface. The window has tabs for Physical, Config, CLI, and Attributes. The Config tab is active. On the left, there is a tree view with categories: GLOBAL, Settings, Algorithm Settings, ROUTING, Static, RIP, SWITCHING, VLAN Database, and INTERFACE. Under the INTERFACE category, Serial0/1/0 is selected. The main area displays the configuration for Serial0/1/0. It includes fields for Port Status (checked On), Duplex (Full Duplex selected), Clock Rate (2000000), IP Configuration (IPv4 Address: 10.0.0.2, Subnet Mask: 255.0.0.0), and Tx Ring Limit (10).

Serial0/1/0	
Port Status	☒ On
Duplex	☒ Full Duplex
Clock Rate	2000000
IP Configuration	
IPv4 Address	10.0.0.2
Subnet Mask	255.0.0.0
Tx Ring Limit	10

iii) Interface S0/1/1

The screenshot shows the configuration window for Router1, specifically for the Serial0/1/1 interface. The left sidebar contains a tree view with categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under the INTERFACE category, the following interfaces are listed: GigabitEthernet0/0, GigabitEthernet0/1, Serial0/1/0, and Serial0/1/1 (which is selected and highlighted in blue). The main configuration area for Serial0/1/1 includes the following settings:

- Port Status:** ☒ On
- Duplex:** ☒ Full Duplex
- Clock Rate:** 2000000
- IP Configuration:**
 - IPv4 Address: 20.0.0.1
 - Subnet Mask: 255.0.0.0
- Tx Ring Limit:** 10

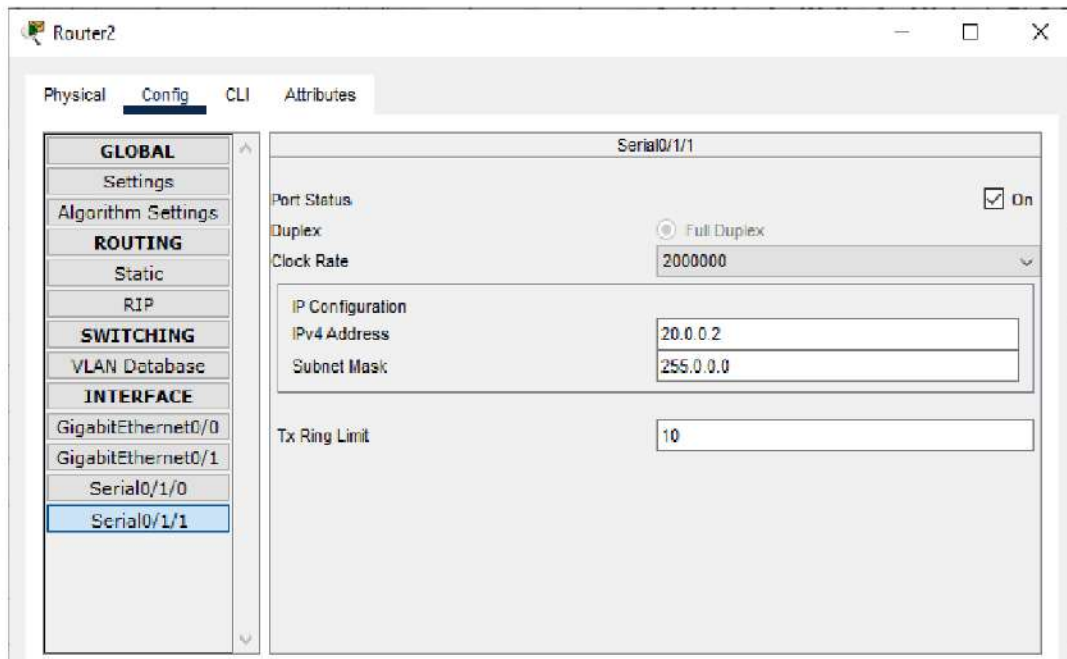
Configuring IP addresses on Router 2

i) Interface G0/0

The screenshot shows the configuration window for Router2, specifically for the GigabitEthernet0/0 interface. The left sidebar contains a tree view with categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under the INTERFACE category, the following interfaces are listed: GigabitEthernet0/0 (which is selected and highlighted in blue), GigabitEthernet0/1, Serial0/1/0, and Serial0/1/1. The main configuration area for GigabitEthernet0/0 includes the following settings:

- Port Status:** ☒ On
- Bandwidth:** ☒ 1000 Mbps ☐ 100 Mbps ☐ 10 Mbps ☒ Auto
- Duplex:** ☒ Half Duplex ☐ Full Duplex ☒ Auto
- MAC Address:** 00D0.FF59.E901
- IP Configuration:**
 - IPv4 Address: 192.168.3.1
 - Subnet Mask: 255.255.255.0
- Tx Ring Limit:** 10

ii) Interface S0/1/1

**Configuring Router 0 for BGP (using the CLI mode)**

```
Router>enable
Router#configure terminal
Router(config)#
Router(config)#router bgp 1000
Router(config-router)#
Router(config-router)#network 10.0.0.0
Router(config-router)#network 192.168.1.0
Router(config-router)#neighbor 10.0.0.2 remote-as 2000
```

Configuring Router 1 for BGP (using the CLI mode)

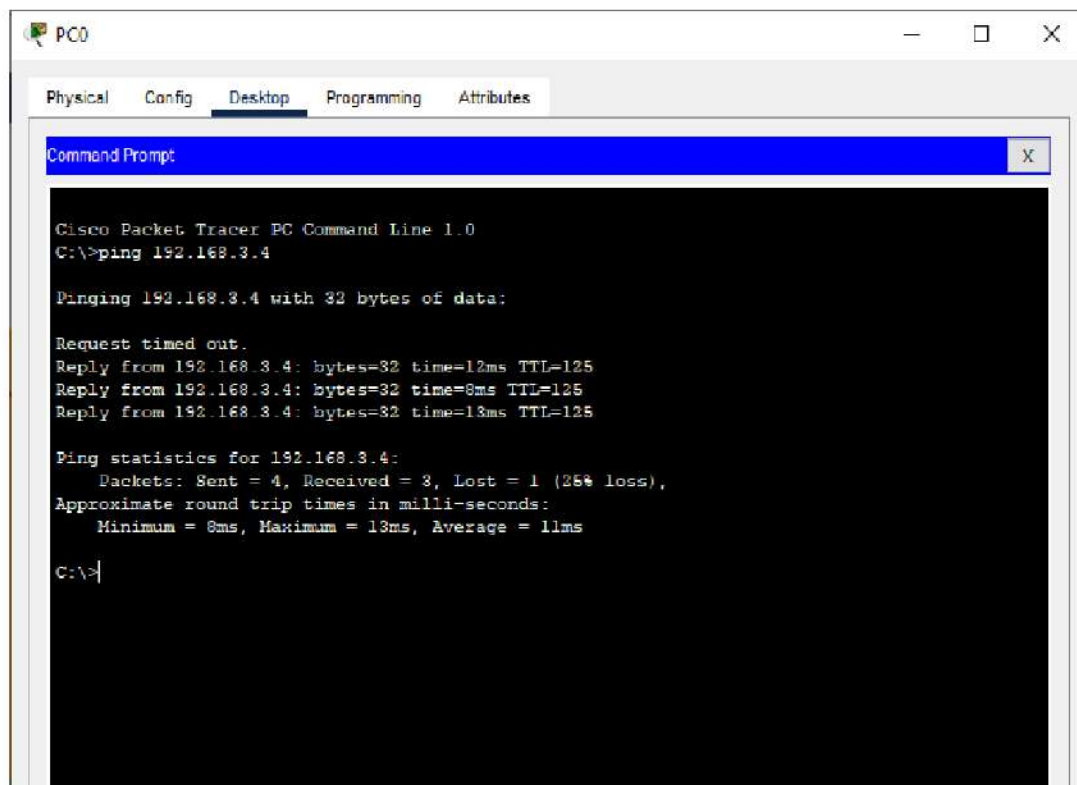
```
Router>enable
Router#configure terminal
Router(config)#
Router(config)#router bgp 2000
Router(config-router)#network 10.0.0.0
Router(config-router)#network 20.0.0.0
Router(config-router)#network 192.168.2.0
Router(config-router)#neighbor 10.0.0.1 remote-as 1000
Router(config-router)#neighbor 20.0.0.2 remote-as 3000
```

Configuring Router 2 for BGP (using the CLI mode)

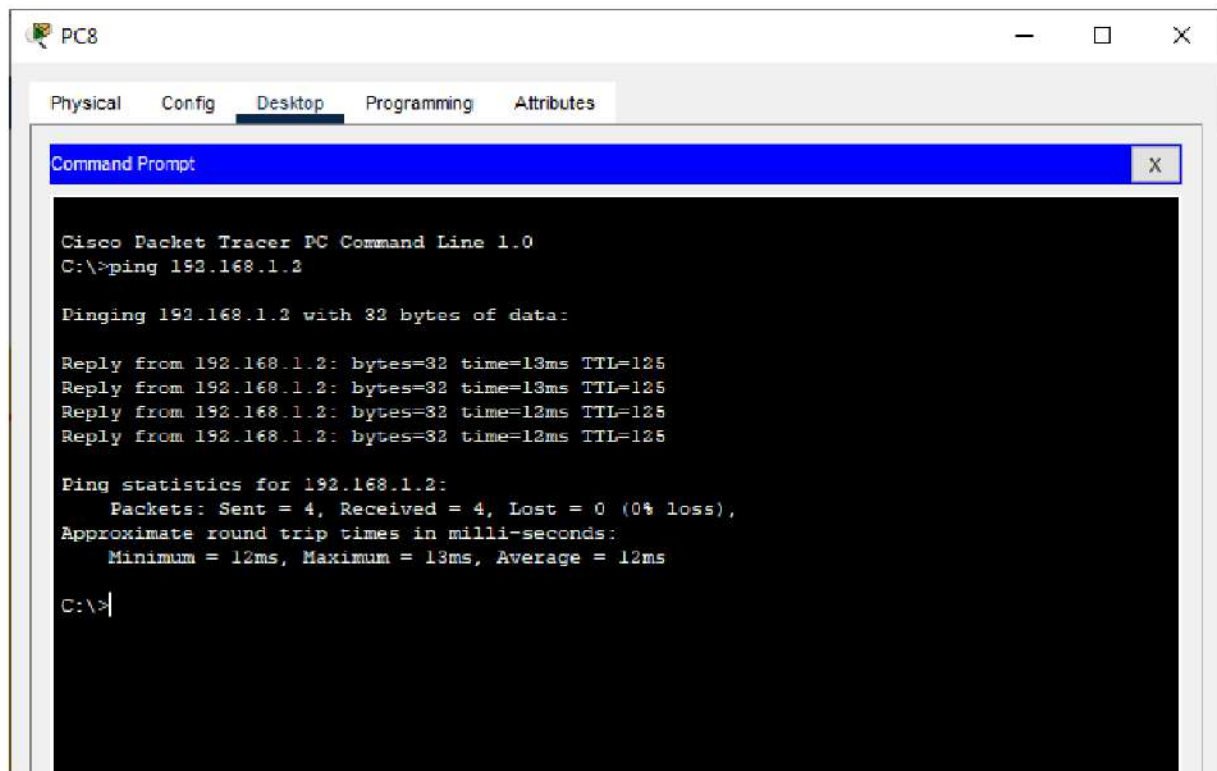
```
Router>enable
Router#configure terminal
Router(config)#
Router(config)#router bgp 3000
Router(config-router)#
Router(config-router)#network 20.0.0.0
Router(config-router)#network 192.168.3.0
Router(config-router)#neighbor 20.0.0.1 remote-as 2000
```

Checking the connectivity by using the ping command

- i) Pinging PC8 (ip address 192.168.3.4) from PC1



ii) Pinging PC0 (ip address 192.168.1.2) from PC8



```
PC8
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=13ms TTL=125
Reply from 192.168.1.2: bytes=32 time=13ms TTL=125
Reply from 192.168.1.2: bytes=32 time=12ms TTL=125
Reply from 192.168.1.2: bytes=32 time=13ms TTL=125

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 13ms, Average = 12ms

C:\>
```

Result:

Hence the BGP has been studied and verified through the given network

Click on the link or scan the QR-code for the video demonstration of the practical:

<https://youtu.be/fBEFfW-TWec>



Practical No 9

Aim: Using Packet Tracer, create a wireless network of multiple PCs using appropriate access point

Theory:

A Wireless Access Point (WAP) is a networking device that allows connecting the devices with the wired network. A Wireless Access Point (WAP) is used to create the WLAN (Wireless Local Area Network), it is commonly used in large offices and buildings which have expanded businesses.

A wireless AP connects the wired networks to the wireless client. It eases access to the network for mobile users which increases productivity and reduces the infrastructure cost.

Advantages of Wireless Access Point (WAP):

- 1) More User Access
- 2) Broader Transmission Range
- 3) Flexible Networking

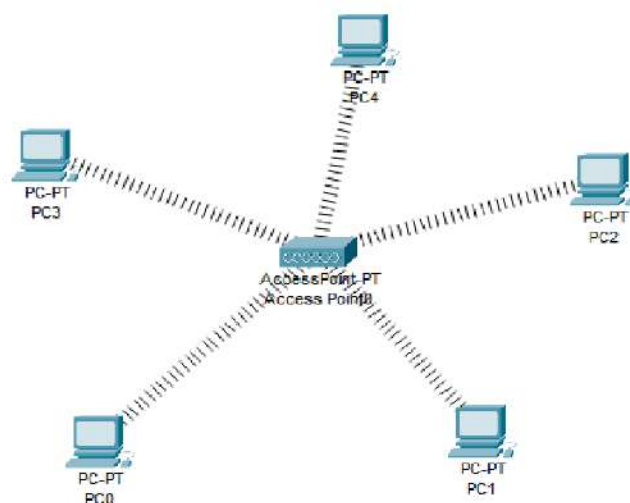
Disadvantages of Wireless Access Point (WAP):

- 1) High cost
- 2) Poor stability
- 3) Less Secure

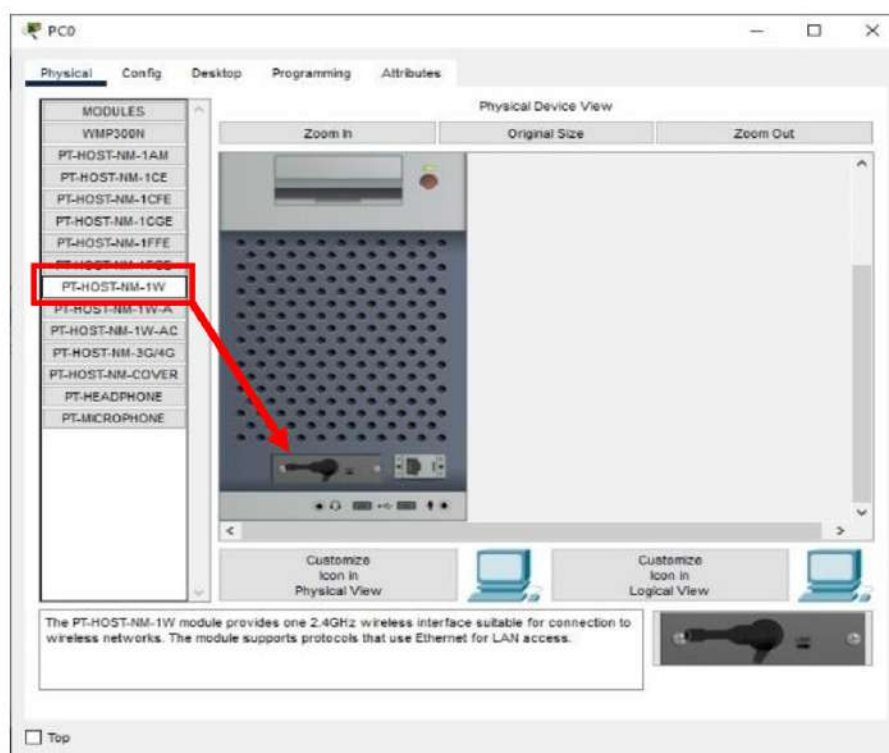
Application of Wireless Access Point:

- 1) It is a device that creates a WLAN (Wireless Local Area Network) in large enterprises.
- 2) It is used to extend the coverage area of the network so that it can't disconnect which allows more users to connect to the network easily.
- 3) An access point connects a switch, Ethernet cable, wired router, and Wi-fi to designate the particular area.
- 4) It is used to provide connectivity to the users in large offices or enterprises which allows users to roam easily anywhere in the office and be connected to a network.
- 5) LANs can also be provided in public places such as coffee shops, restaurants, airports, etc.

We use the following topology for the present case (5PCs and an Access Point)

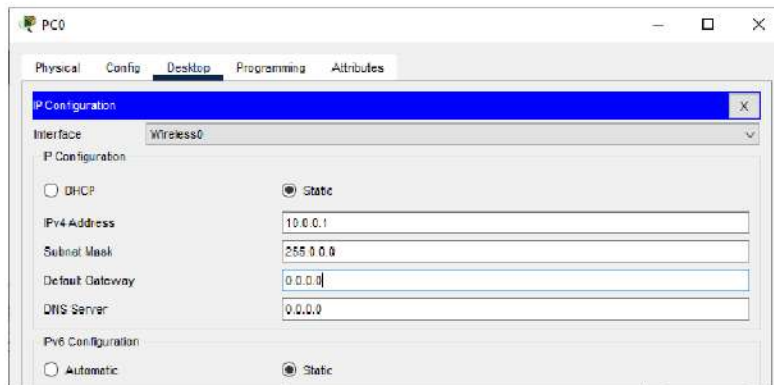


Add a Wireless interface to each PC as follows

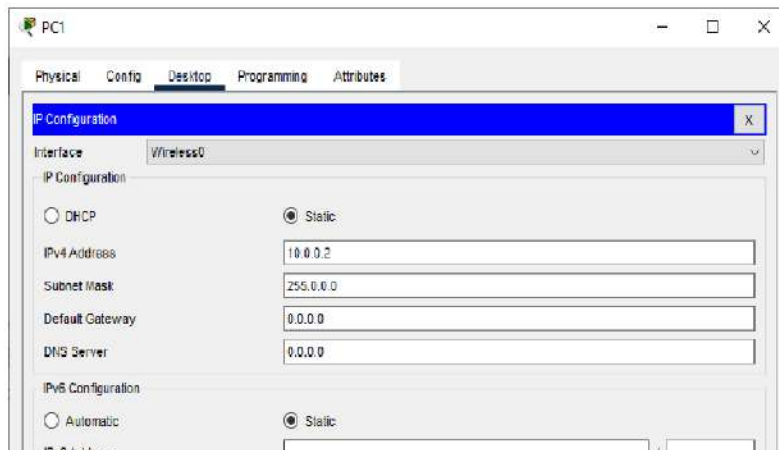


Assigning IP Address to each PC (select Static)

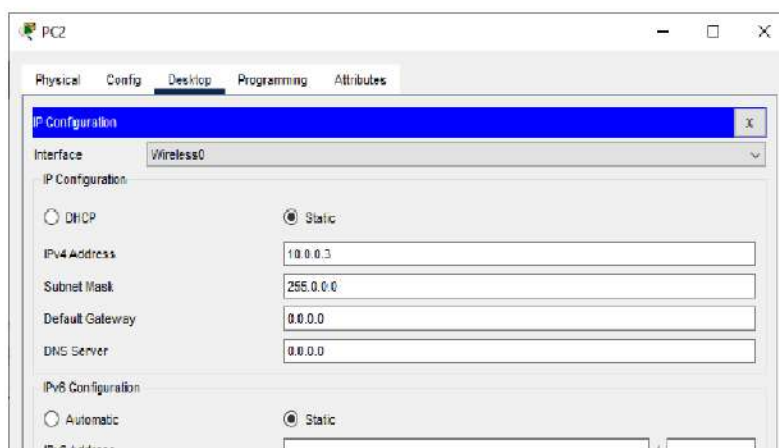
1) PC0 :



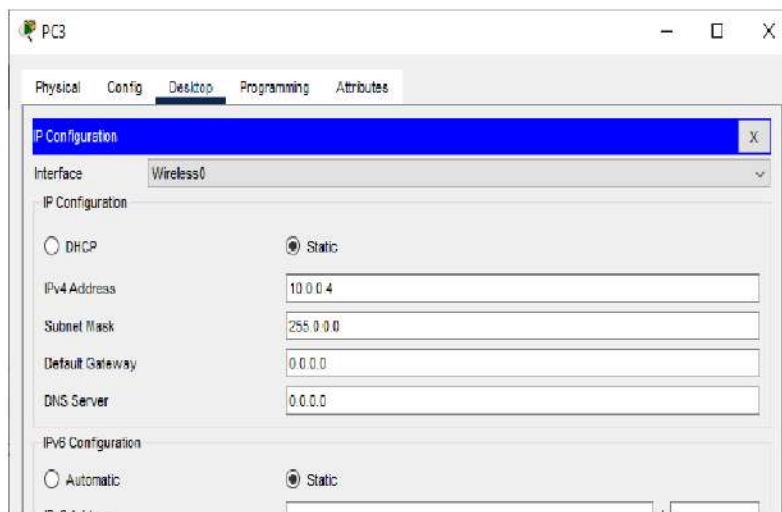
2) PC1 :



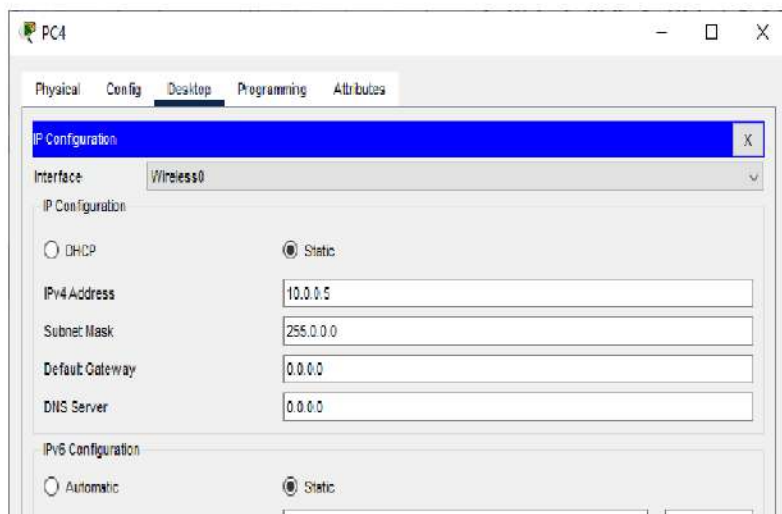
3) PC2 :



4) PC3 :



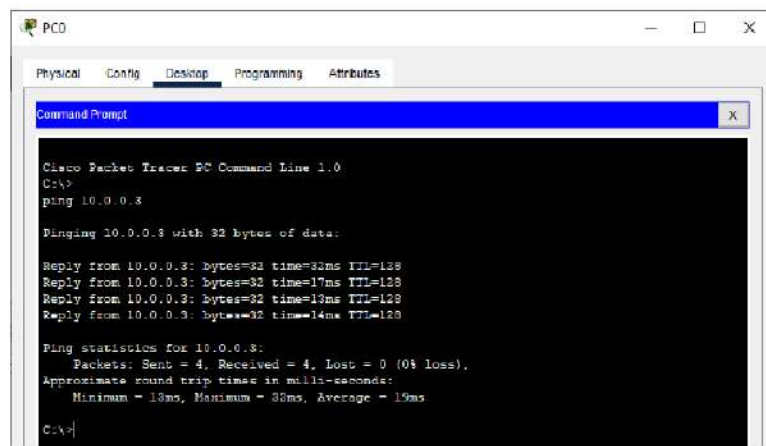
5) PC4 :



The IP addresses assigned are

Host	IP address
PC0	10.0.0.1
PC1	10.0.0.2
PC2	10.0.0.3
PC3	10.0.0.4
PC4	10.0.0.5

We verify the connectivity by sending ping message from any PC to any other PC
 Pinging PC2 (10.0.0.3) from PC0 (10.0.0.1)



```

PC0
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>
ping 10.0.0.3

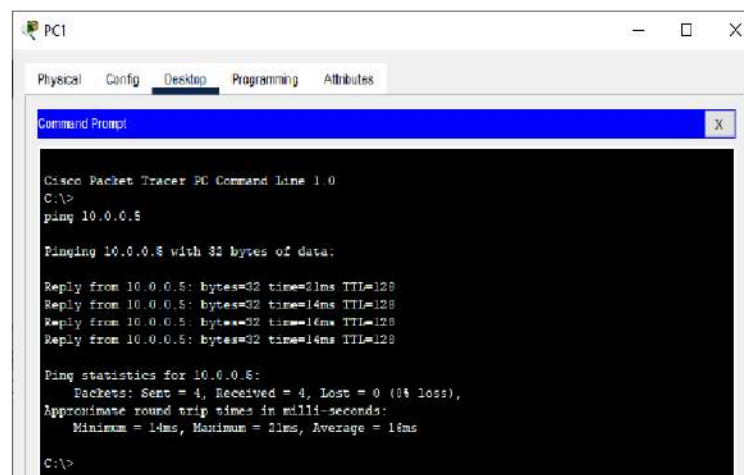
Pinging 10.0.0.3 with 32 bytes of data:

Reply from 10.0.0.3: bytes=32 time=30ms TTL=128
Reply from 10.0.0.3: bytes=32 time=17ms TTL=128
Reply from 10.0.0.3: bytes=32 time=13ms TTL=128
Reply from 10.0.0.3: bytes=32 time=14ms TTL=128

Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 30ms, Average = 19ms

C:\>
  
```

Pinging PC4 (10.0.0.5) from PC1 (10.0.0.2)



```

PC1
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>
ping 10.0.0.5

Pinging 10.0.0.5 with 32 bytes of data:

Reply from 10.0.0.5: bytes=32 time=21ms TTL=128
Reply from 10.0.0.5: bytes=32 time=14ms TTL=128
Reply from 10.0.0.5: bytes=32 time=16ms TTL=128
Reply from 10.0.0.5: bytes=32 time=14ms TTL=128

Ping statistics for 10.0.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 21ms, Average = 16ms

C:\>
  
```

Click on the link or scan the QR-code for the video demonstration of the practical:

<https://youtu.be/c91hCh01DCA>

